STIC EIC 2100 Search Request Form

123328

(3)

Today's Date: 6/1/04

What date would you like to use to limit the search?

Priority Date: NOV 28, 2000 Other:

Name Minh D. Nguyen

AU 2137 Examiner # ~~30~~ 79995

Room # PK2 4R20 Phone 3059727

Serial # 09/724873

Format for Search Results (Circle One):

PAPER DISK EMAIL

Where have you searched so far?

USP DWPI EPO JPO ACM IBM TDB

IEEE INSPEC SPI Other ~~EAST~~

Is this a "Fast & Focused" Search Request? (Circle One) YES NO

A "Fast & Focused" Search is completed in 2-3 hours (maximum). The search must be on a very specific topic and meet certain criteria. The criteria are posted in EIC2100 and on the EIC2100 NPL Web Page at http://ptoweb/patents/stic/stic-tc2100.htm.

What is the topic, novelty, motivation, utility, or other specific details defining the desired focus of this search? Please include the concepts, synonyms, keywords, acronyms, definitions, strategies, and anything else that helps to describe the topic. Please attach a copy of the abstract, background, brief summary, pertinent claims and any citations of relevant art you have found.

an encryptom key stored in a PLD (programmable logic device)
- a plurality of key bits (I found it).
- at least one bit for indicating whether more keys will follow.

STIC Searcher Teresa Osterhold Phone 308-7795

Date picked up 6/1/04 10:45 ~~AM~~ Date Completed 6/1/04 2:00 pm

Search and Information Resources Administration

STIC Search Results Feedback Form

EIC 2100

Questions about the scope or the results of the search? Contact ***the EIC searcher or contact:***

Anne Hendrickson, EIC 2100 Team Leader
308-7831, CPK2-4B40

Voluntary Results Feedback Form

- *I am an examiner in Workgroup:* ☐ *Example: 2133*
- *Relevant prior art **found**, search results used as follows:*
  - ☐ 102 rejection
  - ☐ 103 rejection
  - ☐ Cited as being of interest.
  - ☐ Helped examiner better understand the invention.
  - ☐ Helped examiner better understand the state of the art in their technology.

  Types of relevant prior art found:
  - ☐ Foreign Patent(s)
  - ☐ Non-Patent Literature
    (journal articles, conference proceedings, new product announcements etc.)
- *Relevant prior art **not found:***
  - ☐ Results verified the lack of relevant prior art (helped determine patentability).
  - ☐ Results were not useful in determining patentability or understanding the invention.

Comments:

Drop off or send completed forms to STIC/EIC2100 CPK2-4B40

Set	Items	Description
S1	2387	ENCRYPTION()(KEY OR KEYS)
S2	1461555	STORED OR BACKUP OR BACK()UP OR STORAGE
S3	2666	PLD OR PROGRAMMABLE()LOGIC()DEVICE?
S4	348	(KEY OR KEYS)(N)(BIT OR BITS OR BITE OR BITES OR BYTES)
S5	2890626	INDICAT? OR DETERMIN? OR SPECIF? OR SIGNIF?
S6	1081	(MORE OR FURTHER OR ADDITIONAL)(N)(KEY OR KEYS)
S7	1508049	FOLLOW? OR SUCCEED? OR NEXT OR SUBSEQUENT?
S8	2	S1 AND S2 AND S3
S9	0	S4 AND S5 AND S6
S10	52	S4 AND S5
S11	5	S4 AND S6
S12	5	S10 AND S7
S13	0	S11 AND S7
S14	12	S8 OR S11 OR S12

File 347:JAPIO Nov 1976-2004/Jan(Updated 040506)
(c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200434
(c) 2004 Thomson Derwent

14/5/4 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014967426 **Image available**
WPI Acc No: 2003-027940/200302
XRPX Acc No: N03-021843
Programmable logic device e.g. FPGA comprises voltage level shift circuit for connecting either battery pad or external power supply to key memory registers
Patent Assignee: XILINX INC (XILI-N)
Inventor: ALFKE P H; FRAKE S O; GOETTING F E; KONDAPALLI V M; PANG R C; SHIMANEK S E; SOWARDS J W; WONG J
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6441641	B1	20020827	US 2000724735	A	20001128	200302	B

Priority Applications (No Type Date): US 2000724735 A 20001128 Date not good
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6441641	B1		28	H01L-025/00	

Abstract (Basic): US 6441641 B1
NOVELTY - A switching circuit (22) comprises a voltage level shift circuit for connecting either a battery pad or an external power supply to the memory registers (23b) storing **encryption key**.
USE - **Programmable logic device** e.g. field programmable gate array (FPGA).
ADVANTAGE - Prevents data loss and protects from unauthorized use, by eliminating the need of non-volatile memory and providing **backup** power supply.
DESCRIPTION OF DRAWING(S) - The figure shows the structure of the key memory.
Switching circuit (22)
Memory registers (23b)
pp; 28 DwgNo 10a/16
Title Terms: PROGRAM; LOGIC; DEVICE; COMPRISE; VOLTAGE; LEVEL; SHIFT; CIRCUIT; CONNECT; BATTERY; PAD; EXTERNAL; POWER; SUPPLY; KEY; MEMORY; REGISTER
Derwent Class: U13; U21
International Patent Class (Main): H01L-025/00
File Segment: EPI

14/5/5 (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014865187 **Image available**
WPI Acc No: 2002-685893/200274
XRPX Acc No: N02-541478
Key generation device e.g. for elliptical curvilinear encryption, chooses key generation system based on key selection limit, maximum key bit **length and time for calculation** specified **by user for generating the key**
Patent Assignee: TOSHIBA KK (TOKE)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2002207425	A	20020726	JP 20014043	A	20010111	200274	B

Priority Applications (No Type Date): JP 20014043 A 20010111
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2002207425	A		17	G09C-001/00	

Abstract (Basic): JP 2002207425 A

NOVELTY - The key generation device has a choice unit to choose a key generation system based on key selection limit, maximum **key bit** length and time duration for calculation **specified** by a user. The key is generated by a key generation unit based on the choice result.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the **following** :

(1) Key generation method; and

(2) Public-key encryption program.

USE - For public key encryptions such as elliptical curvilinear encryption, RSA-cipher.

ADVANTAGE - Formation of public key pair of public key encryption is enabled easily and reliably.

DESCRIPTION OF DRAWING(S) - The figure is the block diagram showing the structure of the key generation device.

pp; 17 DwgNo 1/10

Title Terms: KEY; GENERATE; DEVICE; ELLIPSE; CURVE; ENCRYPTION; CHOICE; KEY ; GENERATE; SYSTEM; BASED; KEY; SELECT; LIMIT; MAXIMUM; KEY; BIT; LENGTH; TIME; CALCULATE; **SPECIFIED** ; USER; GENERATE; KEY

Derwent Class: P85; T01

International Patent Class (Main): G09C-001/00

International Patent Class (Additional): G06F-017/10

File Segment: EPI; EngPI

14/5/6 (Item 6 from file: 350)

DIALOG(R)File 350:Derwent WPIX

014214666 **Image available**

WPI Acc No: 2002-035364/200205

XRPX Acc No: N02-027077

Educational toy has plate with questions and answers and guide openings and has key that is fitted into answer, with arrangement of marks to determine if answer is correct

Patent Assignee: LOEWE VERLAG GMBH (LOEW-N)

Inventor: GONDROM V

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 10031546	C1	20020103	DE 1031546	A	20000602	200205	B

Priority Applications (No Type Date): DE 1031546 A 20000602

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 10031546	C1		11	G09B-003/12	

Abstract (Basic): DE 10031546 C1

NOVELTY - The toy has at least one plate (1) with a front side having a question (4) and several answers (5-7), a back side (3) and several guide openings (8-10), each with a different visible mark. A key with a bit fits in the front side of each guide opening and projects through the back plate, so that a mark on the bit lies **next** to the mark on the plate.

DETAILED DESCRIPTION - A key has a bit, which can be fitted in the front side of each guide opening and projects through the back plate by a section, which is a different side for each opening. The **key bit** has a mark corresponding to the marks on the plate. When the key is inserted in an opening, the projecting section lies **next** to a mark, which is different for each opening that the key can be inserted into. The marks only match properly, if the key is inserted into the guide opening with the correct opening.

USE - Educational use.

ADVANTAGE - Expensive correction device is not required.

DESCRIPTION OF DRAWING(S) - The figure shows a schematic view of the front side of a plate of the toy.

Plate (1)

Front side (2)
Question field (4)
Answer fields (5-7)
Guide openings (8-10)
pp; 11 DwgNo 1/9
Title Terms: EDUCATION; TOY; PLATE; QUESTION; ANSWER; GUIDE; OPEN; KEY; FIT ; ANSWER; ARRANGE; MARK; **DETERMINE** ; ANSWER; CORRECT
Derwent Class: P85
International Patent Class (Main): G09B-003/12
File Segment: EngPI

14/5/7 (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

013407196 **Image available**
WPI Acc No: 2000-579134/200054
XRPX Acc No: N00-428591
Programmable logic device **e.g. field programmable gate array, has configuration logic whose input and output terminals are connected to decryptor output terminal and array respectively to receive configuration data**
Patent Assignee: XILINX INC (XILI-N)
Inventor: TRIMBERGER S M
Number of Countries: 021 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200049717	A2	20000824	WO 2000US1398	A	20000119	200054	B
EP 1153480	A2	20011114	EP 2000911598	A	20000119	200175	
			WO 2000US1398	A	20000119		
JP 2002537709	W	20021105	JP 2000600352	A	20000119	200304	
			WO 2000US1398	A	20000119		
EP 1153480	B1	20030402	EP 2000911598	A	20000119	200325	
			WO 2000US1398	A	20000119		
DE 60001927	E	20030508	DE 601927	A	20000119	200338	
			EP 2000911598	A	20000119		
			WO 2000US1398	A	20000119		
US 6654889	B1	20031125	US 99253401	A	19990219	200378	

Priority Applications (No Type Date): US 99253401 A 19990219
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200049717	A2	E	23	H03K-019/00	
Designated States (National): JP					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
EP 1153480	A2	E		H03K-019/00	Based on patent WO 200049717
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
JP 2002537709	W		24	H04L-009/10	Based on patent WO 200049717
EP 1153480	B1	E		H03K-019/00	Based on patent WO 200049717
Designated States (Regional): DE FR GB					
DE 60001927	E			H03K-019/00	Based on patent EP 1153480
					Based on patent WO 200049717
US 6654889	B1			H04L-009/32	

Abstract (Basic): WO 200049717 A2
NOVELTY - A decryptor (350) decrypts the encrypted configuration data received through input terminal, for accessing decryption key **stored** in RAM (310) through other input terminal and outputs the decrypted data to output terminal connected to input of configuration logic (305). Output of configuration logic is coupled to array (315) which is configured based on configuration data received by configuration logic.
DETAILED DESCRIPTION - The logic device comprises hash-function logic for authenticating portion of decryptor. A non-volatile memory

element is coupled to hash-function logic to store hash key and **encryption key** . INDEPENDENT CLAIMS are also included for the following:

(a) configuration data protecting system;

(b) **programmable logic device** configuring method

USE - In e.g. field programmable gate array (FPGA) using encrypted configuration data.

ADVANTAGE - The configuration data are used to instantiate the decryptor, for overcoming the security breach and only configuration data of decryptor produces the desired hash result that has access to decryption key which cannot be operated by unknown person, thus protecting data from theft.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of FPGA.

Configuration logic (305)

RAM (310)

Array (315)

Decryptor (350)

pp; 23 DwgNo 3/6

Title Terms: PROGRAM; LOGIC; DEVICE; FIELD; PROGRAM; GATE; ARRAY; CONFIGURATION; LOGIC; INPUT; OUTPUT; TERMINAL; CONNECT; OUTPUT; TERMINAL; ARRAY; RESPECTIVE; RECEIVE; CONFIGURATION; DATA

Derwent Class: P85; U21

International Patent Class (Main): H03K-019/00; H04L-009/10; H04L-009/32

International Patent Class (Additional): G09C-001/00

File Segment: EPI; EngPI

14/5/8 (Item 8 from file: 350)

DIALOG(R)File 350:Derwent WPIX

011334667 **Image available**

WPI Acc No: 1997-312571/199729

XRPX Acc No: N97-258820

Key cutting machine for cutting defined bit notch pattern in key blank - has mode control operating machine in either analog mode where blank is cut by following pattern of master key, or mode where digital data signal is used to replicate key pattern

Patent Assignee: AXXESS TECHNOLOGIES INC (AXXE-N)

Inventor: CARLSON B D; HEREDIA G L; MUELLER M A

Number of Countries: 008 Number of Patents: 010

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 779120	A1	19970618	EP 96118450	A	19961118	199729	B
AU 9675305	A	19970619	AU 9675305	A	19961211	199733	
CA 2169142	A	19970615	CA 2169142	A	19960208	199742	
JP 9216112	A	19970819	JP 96335903	A	19961216	199743	
US 5676504	A	19971014	US 95572766	A	19951214	199747	
AU 686055	B	19980129	AU 9675305	A	19961211	199812	
JP 3001444	B2	20000124	JP 96335903	A	19961216	200009	
CA 2169142	C	20000822	CA 2169142	A	19960208	200052	
EP 779120	B1	20021030	EP 96118450	A	19961118	200272	
DE 69624547	E	20021205	DE 624547	A	19961118	200304	
			EP 96118450	A	19961118		

Priority Applications (No Type Date): US 95572766 A 19951214

Cited Patents: CH 673612

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 779120	A1	E	29	B23C-003/35	
Designated States (Regional): DE FR GB IT					
AU 9675305	A			B23C-003/35	
CA 2169142	A			B23C-003/30	
JP 9216112	A		21	B23C-003/35	
US 5676504	A		32	B23C-001/16	
AU 686055	B			B23C-003/35	Previous Publ. patent AU 9675305

JP 3001444 B2 20 B23C-003/35 Previous Publ. patent JP 9216112
CA 2169142 C E B23C-003/30
EP 779120 B1 E B23C-003/35
Designated States (Regional): DE FR GB IT
DE 69624547 E B23C-003/35 Based on patent EP 779120

Abstract (Basic): EP 779120 A

The key cutting machine (10) includes a cutter wheel and a key **follower** spaced for it. A mode control system selectively configures machine to operate in either analog mode or digital mode. In analog mode key **follower** engages master **key bit** notch pattern and displaces cutter wheel and key blank to mechanically trace and duplicate master key pattern in blank.

In a digital mode, a cutter wheel is displaced relative to the blank in response to digital data signal as cutter wheel and blank are moved relative to each other to electronically duplicate defined pattern in blank blade without reference to master pattern.

Dwg.1A/36

Title Terms: KEY; CUT; MACHINE; CUT; DEFINE; BIT; NOTCH; PATTERN; KEY; BLANK; MODE; CONTROL; OPERATE; MACHINE; ANALOGUE; MODE; BLANK; CUT; **FOLLOW** ; PATTERN; MASTER; KEY; MODE; DIGITAL; DATA; SIGNAL; REPLICA; KEY; PATTERN
Derwent Class: P54; P56; X25
International Patent Class (Main): B23C-001/16; B23C-003/30; B23C-003/35
International Patent Class (Additional): B23D-001/00; B23D-013/00; B23Q-035/00; B23Q-035/10
File Segment: EPI; EngPI

14/5/9 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010354627 **Image available**
WPI Acc No: 1995-255941/199534
XRPX Acc No: N95-197529

Electromagnetically operated security lock esp. for safe-deposit doors - includes slotted tumblers engaged by fixed pin on sliding bolt for two-stage switching of electromagnet during unlocking by proper key

Patent Assignee: STEINBACH & VOLLMANN (STEI-N)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 4420747	C1	19950727	DE 4420747	A	19940615	199534	B

Priority Applications (No Type Date): DE 4420747 A 19940615
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 4420747	C1		11	E05B-047/06	

Abstract (Basic): DE 4420747 C

The bolt (2) incorporates a slot (2b) where it can be retracted by means of a key (S) subject to correct positioning of tumblers (3,3'), pivotable about a spike (4) on the floor (1a) of the casing (1) and co-operating with a fixed pin (2c).

The bolt is also secured by a pref. battery-powered electromagnet (5) provided with two microswitches (7a,7b) to reduce its current consumption. The first microswitch (7a) is closed by a lever (9) operated by a **key bit** at the beginning of rotation of the **key** . **Further** rotation opens the second microswitch (7b) after the pin has entered the slots (3b) in the tumblers.

ADVANTAGE - The current required for unlocking is reduced substantially by simple and inexpensive switching with complete security.

Dwg.1/9

Title Terms: ELECTROMAGNET; OPERATE; SECURE; LOCK; SAFE; DEPOSIT; DOOR; SLOT; TUMBLE; ENGAGE; FIX; PIN; SLIDE; BOLT; TWO; STAGE; SWITCH;

ELECTROMAGNET; UNLOCK; PROPER; KEY
Derwent Class: Q47; X25
International Patent Class (Main): E05B-047/06
International Patent Class (Additional): E05B-035/12
File Segment: EPI; EngPI

14/5/10 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX

009408972 **Image available**
WPI Acc No: 1993-102483/199313
XRPX Acc No: N93-077899

Number-plate-fixing device inside plastics guard - comprises keys inserted and turned in keyholes in baseplate

Patent Assignee: PEUKER G (PEUK-I); PEUKER T (PEUK-I)
Inventor: PEUKER G; PEUKER T
Number of Countries: 016 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 534315	A1	19930331	EP 92115913	A	19920917	199313	B
DE 4132267	A1	19930408	DE 4132267	A	19910927	199315	
CZ 9202926	A3	19930414	CS 922926	A	19920924	199332	N
DE 4132267	C2	19940224	DE 4132267	A	19910927	199408	
SK 9202926	A3	19940810	CS 922926	A	19920924	199436	
EP 534315	B1	19950510	EP 92115913	A	19920917	199523	
HU 68295	T	19950628	HU 923058	A	19920925	199532	

Priority Applications (No Type Date): DE 4132267 A 19910927; CS 922926 A 19920924
Cited Patents: DE 2306782; DE 8912546; DE 9015713; DE 9106115
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 534315	A1	G	7	B60R-013/10	
Designated States (Regional): AT BE CH ES FR GB GR IT LI NL PT					
DE 4132267	A1		5	B60R-013/10	
DE 4132267	C2		5	B60R-013/10	
EP 534315	B1	G	7	B60R-013/10	
Designated States (Regional): AT BE CH ES FR GB GR IT LI NL PT					
CZ 9202926	A3			G09F-007/18	
SK 9202926	A3			G09F-007/00	
HU 68295	T			B60R-013/10	

Abstract (Basic): EP 534315 A

The fixing device secures a numberplate inside a plastics reinforcing guard. The latter comprises a baseplate (2) with standard fixing holes as used for a vehicle, and a peripheral channel-section edge (3) with a deeper rib (4) fitting over the numberplate edge. Along one side, the edge is wider than elsewhere, forming a detachable covering strip over fixing devices.

The baseplate contains openings (6) with keyholes (7) for keys (8) bent over on the baseplate. Each key has a flat oval head (9) with an eccentric shank (10) on one side. On the end of the shank are one or more tongues (11), it being inserted and turned in the keyhole. Ribs (12) on the underside of the covering strip (5) then lock the head in the engaged position.

USE/ADVANTAGE - Rapid, easy and sure fixing of numberplate so that it will not rattle.

Dwg.1-4/4

Title Terms: NUMBER; PLATE; FIX; DEVICE; PLASTICS; GUARD; COMPRISE; KEY; INSERT; TURN; KEYHOLE; BASEPLATE
Derwent Class: P85; Q17
International Patent Class (Main): B60R-013/10; G09F-007/18
File Segment: EngPI

14/5/11 (Item 11 from file: 350)
DIALOG(R)File 350:Derwent WPIX

007288400
WPI Acc No: 1987-285407/198741
Safety lock with either side-lockable double cylinders - has outside- and inside cylinders with drop locking pins and key bit **bore containing spring loaded blocks**
Patent Assignee: EFUNE E (EFUN-I)
Inventor: EFUNE E
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 3632663	A	19871008				198741	B

Priority Applications (No Type Date): DE 632663 A 19860926
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 3632663	A		6		

Abstract (Basic): DE 3632663 A
The safety lock with either side-lockable double cylinders consists of outside cylinder assembly (1) with drop locking pins, inside cylinder assembly (3) with drop locking pins (2), limiting disc (4) engaging with grooves provided in the cylinders, **further key bit** assembly (5) mounted between the outside cylinder and the inside cylinder. All the above assemblies are accommodated in housing (10).
The **key bit** has bore in which sliding blocks (6,6a) are mounted with key-accepting slots. The two blocks are kept apart by spring (8).
ADVANTAGE - The mechanism allows operation of one cylinder without interference from the other cylinder. This operation can be carried out even if the key is left in the lock on either side of the mechanism.
(6pp Dwg.No2/9
Derwent Class: Q47
International Patent Class (Main): E05B-009/10
International Patent Class (Additional): E05B-027/00
File Segment: EngPI

14/5/12 (Item 12 from file: 350)
DIALOG(R)File 350:Derwent WPIX

003864918
WPI Acc No: 1984-010445/198402
XRPX Acc No: N84-007535
Key operated coded lock - has two-part core with spring-loaded locking pins in one part and main key hole in other part
Patent Assignee: USIKOV A N (USIK-I)
Inventor: USIKOV N V
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
SU 1002489	A	19830307	SU 3003466	A	19801113	198402	B

Priority Applications (No Type Date): SU 3003466 A 19801113
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
SU 1002489	A		8		

Abstract (Basic): SU 1002489 A
The lock has housing (1), core (2), crosspiece (3), key (4) and lower (5) and upper (6) locking pins. Crosspiece (3) engages with pinions (7), and limiters are secured to pins (6) and interact with guide pinions mounted on shaft (10). These limiters have false grooves (11), working grooves and teeth (13) which engage with number discs

(14). Disc (14) are mounted on shaft (15) and have teeth (16) and spring (17). The discs are brought into motion by spring-loaded forks.

The forks

have wedges (21) mounted on a strut. Wedges (21) can interact via bit (23) with **additional key** (24). Core (2) consists of housing (25) and segmented section (26). Main key (4) is formed by rod (28) of a guide in which the **key bit** , consisting of plates (30), is installed. Plate spring (31) is hinged to rod (28). To replace core (2) there is cap (32) and wedge guide (33), and the limiters have stops (34).

The lock can be used for doors and safes, and it has a numerical code and a code provided by main key (4). The code is set with key (4) and by turning key (24) to free numerical discs (14). The number of operations for unlocking is minimal and the lock has increased secrecy.

Bul.9/7.3.83

(8pp Dwg.No.1/5

Title Terms: KEY; OPERATE; CODE; LOCK; TWO-PART; CORE; SPRING; LOAD; LOCK; PIN; ONE; PART; MAIN; KEY; HOLE; PART

Derwent Class: Q47

International Patent Class (Additional): E05B-037/20

File Segment: EngPI

```
Set     Items   Description
S1       5277   ENCRYPTION()(KEY OR KEYS)
S2     525155   STORED OR BACKUP OR BACK()UP OR STORAGE
S3       4799   PLD OR PROGRAMMABLE()LOGIC()DEVICE?
S4       1203   (KEY OR KEYS)(N)(BIT OR BITS OR BITE OR BITES OR BYTES)
S5    1322295   INDICAT? OR DETERMIN? OR SPECIF? OR SIGNIF?
S6       4174   (MORE OR FURTHER OR ADDITIONAL)(N)(KEY OR KEYS)
S7    1188351   FOLLOW? OR SUCCEED? OR NEXT OR SUBSEQUENT?
S8          5   S1 (S) S2 (S) S3
S9         18   S4 (S) S5 (S) S6
S10        13   S9 (S) S7
S11        18   S8 OR S10
File 348:EUROPEAN PATENTS 1978-2004/May W04
         (c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040527,UT=20040520
         (c) 2004 WIPO/Univentio
```

11/5,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00712015

A SECURE MEMORY CARD WITH PROGRAMMED CONTROLLED SECURITY ACCESS CONTROL
GESICHERTE SPEICHERKARTE MIT PROGRAMMIERTER GESTEUERTER SICHERHEITS-ZUGRIFF S-KONTROLLE
CARTE A MEMOIRE SECURISEE A COMMANDE D'ACCES DE SECURITE COMMANDEE PROGRAMMEE

PATENT ASSIGNEE:
CP8 TRANSAC, (1983110), 68, Route de Versailles, BP 45, F-78430 Louveciennes, (FR), (Proprietor designated states: all)
INVENTOR:
HOLTEY, Thomas, O., 10 Crehore Drive, Newton, MA 02162, (US)
LEGAL REPRESENTATIVE:
Corlu, Bernard Edouard et al (60534), SchlumbergerSema Direction de la Propriete Intellectelle 36-38, rue de la Princesse - B.P. 45, 78431 Louveciennes, (FR)

PATENT (CC, No, Kind, Date): EP 689701 A1 960103 (Basic)
EP 689701 B1 011212
WO 9519607 950720
APPLICATION (CC, No, Date): EP 95904673 950112; WO 95IB27 950112
PRIORITY (CC, No, Date): US 181691 940114
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; NL; PT; SE
INTERNATIONAL PATENT CLASS: G06K-019/073; G07F-007/10
CITED PATENTS (EP B): EP 115348 A; EP 212615 A; EP 262025 A; EP 596276 A; DE 3636700 A; FR 2611289 A
NOTE:
No A-document published by EPO
LEGAL STATUS (Type, Pub Date, Kind, Text):

Change:	001011 A1	Title of invention (German) changed: 20000824
Application:	950927 A	International application (Art. 158(1))
Lapse:	030226 B1	Date of lapse of European Patent in a contracting state (Country, date): AT 20011212, GR 20011212,
Grant:	011212 B1	Granted patent
Change:	011004 A1	Legal representative(s) changed 20010816
Oppn None:	021204 B1	No opposition filed: 20020913
Lapse:	021204 B1	Date of lapse of European Patent in a contracting state (Country, date): GR 20011212,
Application:	960103 A1	Published application (A1with Search Report ;A2without Search Report)
Examination:	960320 A1	Date of filing of request for examination: 960122
Examination:	980916 A1	Date of despatch of first examination report: 980729

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200150	1761
CLAIMS B	(German)	200150	1580
CLAIMS B	(French)	200150	2051
SPEC B	(English)	200150	7956
Total word count - document A			0
Total word count - document B			13348
Total word count - documents A + B			13348

...SPECIFICATION a binary ZERO to be written into lock bit position LMB0 of the first memory block as **indicated** by block 606 of Figure 6a. As **indicated** in block 608 of Figure 6a, the execution of each step instruction causes a **next** bit of the key value stored in ACP 10 memory to be written into the **next** lock bit location (e.g. LMB1) of the first block. If there are **more key bits** to be written into the lock bit positions of the first block, ACP 10 causes the execution of another step

instruction. Step instructions are executed until the ACP 10 **determines** that all of the bits of the stored key value have been written into the lock bit positions of lock memory area for the first memory block. The ACP 10 makes the **determination** by detecting that 7 consecutive ONES have occurred signaling the end of the key value.

As indicated...

11/5,K/2 (Item 2 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

00544380

Data security arrangements for semiconductor programmable logic devices

Datensicherheitseinrichtungen fur programmierbare logische Halbleiterschaltungen

Appareils de securite de donnees pour des dispositifs logiques programmables semi-conducteurs

PATENT ASSIGNEE:
MOTOROLA, INC., (205770), 1303 East Algonquin Road, Schaumburg, IL 60196, (US), (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT;SE)

INVENTOR:
Austin, Kenneth, Brockhurst Hall, Brockhurst Way, Northwich, Cheshire CW9 8AP, (GB)

LEGAL REPRESENTATIVE:
Williamson, Simeon et al (87201), Motorola European Intellectual Property Operations Midpoint Alencon Link, Basingstoke, Hampshire RG21 7PL, (GB)

PATENT (CC, No, Kind, Date): EP 536943 A2 930414 (Basic)
EP 536943 A3 930616
EP 536943 B1 990707

APPLICATION (CC, No, Date): EP 92308939 920930;

PRIORITY (CC, No, Date): GB 9121591 911011

DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE

INTERNATIONAL PATENT CLASS: G06F-012/14;

CITED PATENTS (EP A): EP 154252 A; EP 154252 A; EP 162707 A; US 4593353 A; EP 238230 A

ABSTRACT EP 536943 A2

A data security arrangement is provided to protect configuration data to be stored in static random access memories (38) in semiconductor programmable logic devices PLD. The configuration data, which is vulnerable to illegal duplication, is normally held in a read only memory ROM, typically an erasable programmable read only memory.

A data coding means is provided to code the configuration data to be loaded to the PLD and a data decoding means is provided in the PLD to decode the coded configuration data. The coding and decoding means each incorporate maximal length shift registers (12, 25) which generate a pseudo-random sequence of bits. A key value is input to the shift register (12) in the coding means forcing it to start at a particular point in the sequence. The output (bits B28 and B31) of this register is combined in an EXCLUSIVE-OR gate (20) with configuration data and coded data is written to the read only memory ROM (24). The decoding means in the PLD has a corresponding key value held in a non-volatile memory (28) in the PLD. This is applied to the register (25) of the decoding means whose output (bits B28 and B31) are combined in an EXCLUSIVE-OR GATE (34) with coded configuration data CDIC read from the ROM (24) to produce decoded configuration data CDOD to be sotred in the memories (38). (see image in original document)

ABSTRACT WORD COUNT: 233

LEGAL STATUS (Type, Pub Date, Kind, Text):

Lapse: 000614 B1 Date of lapse of European Patent in a contracting state (Country, date): AT 19990707, BE 19990707,

Application: 930414 A2 Published application (Alwith Search Report

			;A2without Search Report)
Lapse:	031105	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 19990707, BE 19990707, CH 19990707, LI 19990707, DK 19991007, ES 19990707, GR 19990707, MC 20000331, NL 19990707, PT 19991007, SE 19990707,
Lapse:	030423	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 19990707, BE 19990707, CH 19990707, LI 19990707, ES 19990707, GR 19990707, MC 19990930, NL 19990707, PT 19991007, SE 19990707,
Lapse:	020619	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 19990707, BE 19990707, CH 19990707, LI 19990707, ES 19990707, GR 19990707, MC 20000331, PT 19991007, SE 19990707,
Lapse:	010606	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 19990707, BE 19990707, CH 19990707, LI 19990707, GR 19990707, MC 20000331, PT 19991007,
Lapse:	001213	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 19990707, BE 19990707, CH 19991012, LI 19991012, PT 19991007,
Oppn None:	000628	B1	No opposition filed: 20000408
Lapse:	000628	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 19990707, BE 19990707, PT 19991007,
Lapse:	001227	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 19990707, BE 19990707, CH 19990707, LI 19990707, MC 20000331, PT 19991007,
Lapse:	020605	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 19990707, BE 19990707, CH 19990707, LI 19990707, GR 19990707, MC 20000331, PT 19991007, SE 19990707,
Lapse:	030212	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 19990707, BE 19990707, CH 19990707, LI 19990707, ES 19990707, GR 19990707, MC 20000331, NL 19990707, PT 19991007, SE 19990707,
Lapse:	030502	B1	Date of lapse of European Patent in a contracting state (Country, date): AT 19990707, BE 19990707, CH 19990707, LI 19990707, ES 19990707, GR 19990707, MC 20000331, NL 19990707, PT 19991007, SE 19990707,
Search Report:	930616	A3	Separate publication of the European or International search report
Examination:	931124	A2	Date of filing of request for examination: 930928
Examination:	970528	A2	Date of despatch of first examination report: 970409
Change:	990224	A2	Representative (change)
Change:	990623	A2	Representative (change)
*Assignee:	990623	A2	Applicant (transfer of rights) (change): MOTOROLA, INC. (205770) 1303 East Algonquin Road Schaumburg, IL 60196 (US) (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT ;SE)
*Assignee:	990623	A2	Previous applicant in case of transfer of

rights (change): Pilkington Micro-Electronics Limited (790700) Prescot Road St. Helens Merseyside WA10 3TT (GB) (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT;SE)

Grant: 990707 B1 Granted patent

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9927	759
CLAIMS B	(German)	9927	651
CLAIMS B	(French)	9927	965
SPEC B	(English)	9927	1607
Total word count - document A			0
Total word count - document B			3982
Total word count - documents A + B			3982

...CLAIMS volatile storage means is constituted by static random access memories (38).

14. A method of configuring a **programmable logic device** that includes a semiconductor device having (1) configurable circuitry, (2) an input circuitry (35) for receiving data...

...3) decrypting circuitry (25, 29, 34) connected to said input circuitry (35), (4) a non-volatile data **storage** device (28) connected to said decrypting circuitry (35), and (5) volatile **storage** circuitry (38), which method comprises encrypting configuration data by use of an **encryption key** value, storing said configuration data in said data store (24) after encryption, inputting encrypted data from said data store to said **programmable logic device** , deriving a decryption key value from said non-volatile store (28) in said **programmable logic device** , said decryption key value being the same as said **encryption key** value, decrypting said encrypted data by use of said decrypting key value, storing said data after decryption in said volatile **storage** circuitry (38) in said **programmable logic device** and configuring said **programmable logic device** according to decrypted data in said volatile **storage** circuitry.

11/5,K/3 (Item 3 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

00286763

Apparatus and method for providing digital audio on the sound carrier of a standard television signal.

Vorrichtung und Verfahren zur Herstellung eines digitalen Audiosignals auf dem Tontrager eines Standardfernsehsignals.

Dispositif et procede pour l'obtention d'un signal audio-numerique sur la porteuse de son d'un signal de television standard.

PATENT ASSIGNEE:

GENERAL INSTRUMENT CORPORATION, (264771), 767 Fifth Avenue, New York New York 10153, (US), (applicant designated states: DE;FR;GB)

INVENTOR:

Robbins, Clyde, 1524 Terrace Drive, Maple Glen Pennsylvania 19002, (US)

LEGAL REPRESENTATIVE:

Hoeger, Stellrecht & Partner (100381), Uhlandstrasse 14 c, W-7000 Stuttgart 1, (DE)

PATENT (CC, No, Kind, Date): EP 284799 A2 881005 (Basic)
EP 284799 A3 890920
EP 284799 B1 930721

APPLICATION (CC, No, Date): EP 88103112 880302;

PRIORITY (CC, No, Date): US 22380 870305

DESIGNATED STATES (Pub A): BE; CH; DE; FR; GB; IT; LI; NL; SE; (Pub B): DE; FR; GB

INTERNATIONAL PATENT CLASS: H04N-007/04; H04N-007/10;

CITED PATENTS (EP A): EP 149950 A; EP 149950 A; EP 144770 A; WO 8601967 A; GB 2145610 A; EP 140753 A

CITED REFERENCES (EP A):

INTERNATIONAL BROADCASTING AUTHORITY/ I.B.A., specification M 06.11.87, September 1986, pages 1-20; "Specification of a standard for UK stereo with - television transmissions"

IDEM

IEE PROCEEDINGS, SECTION A a I, vol. 133, no. 4, part F, July 1986, pages 374-383, Stevenage, Herts, GB; J.S. LOTHIAN et al.: "The C-MAC/pacKet system for satellite broadcasting"

IDEM

NHK LABORATORIES NOTE, serial no. 304, September 1984, pages 2-12, NHK, Tokyo, JP; Y. NINOMIYA et al.: "A single channel HDTV broadcast system - the MUSE"

13th INTERNATIONAL TV SYMPOSIUM, Montreux, 28th May - 2nd June 1983, pages 191-200; K. YABASHI: "Technical aspects of satellite broadcasting in Japan"

IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, vol. SAC-3, no. 1, January 1985, pages 135-147, IEEE, New York, US; M. DAVIDOV et al.: "Threshold extension in DBS system design"

IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. CE-30, no. 3, August 1984, pages 265-271, IEEE, New York, US; T. ARAI et al.: "Receiver for DBS with digital audio signals";

ABSTRACT EP 284799 A2

A television transmission system replaces the standard FM audio portion of a television signal with digital audio. Three digital audio channels are time division multiplexed on the sound carrier, using combined multi-phase and AM modulation. The audio signals are digitized using adaptive delta modulation techniques. Video vertical and horizontal framing, as well as the audio carrier phase reference, audio data bit time and frame reference, and various control data is carried using AM modulation. The digital audio information is carried using multi-phase modulation. The composite data stream may be serially encrypted to provide security and prevent unauthorized reproduction of the video and/or audio portions of the television signal.

ABSTRACT WORD COUNT: 112

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	881005	A2	Published application (A1with Search Report ;A2without Search Report)
Change:	890802	A2	Obligatory supplementary classification (change)
Search Report:	890920	A3	Separate publication of the European or International search report
Examination:	900411	A2	Date of filing of request for examination: 900213
Examination:	920415	A2	Date of despatch of first examination report: 920302
Grant:	930721	B1	Granted patent
Oppn None:	940713	B1	No opposition filed

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPBBF1	1688
CLAIMS B	(German)	EPBBF1	1779
CLAIMS B	(French)	EPBBF1	2452
SPEC B	(English)	EPBBF1	9939
Total word count - document A			0
Total word count - document B			15858
Total word count - documents A + B			15858

...SPECIFICATION amplitude or frequency companding data, and the contents of sequential lines alternate from one line to the **next** .

Bits 16-23 of the tag data carry data associated with the digital audio program, and is...

...decryption key prior to evaluation. The two bytes are broken down into four nibbles, each specifically the **appropriate key** nibble to be used in the associated key section. Table 6 indicates the correspondence between the key usage identifier nibbles and the key nibbles. (see image in original document)
This scheme allows **any** key nibble to be used in any section of the key latch.
Another byte of data is...

11/5,K/8 (Item 5 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00910752 **Image available**
PROGRAMMABLE LOGIC DEVICE WITH DECRYPTION ALGORITHM AND DECRYPTION KEY
UNITE LOGIQUE PROGRAMMABLE A ALGORITHME DE DECRYPTAGE ET CLE DE DECRYPTAGE
Patent Applicant/Assignee:
XILINX INC, 2100 Logic Drive, San Jose, CA 95124, US, US (Residence), US (Nationality)
Inventor(s):
PANG Raymond C, 1138 Falcon Ridge Court, San Jose, CA 95120, US,
SZE Walter N, 20439 Kirkmont Drive, Saratoga, CA 95070, US,
WONG Jennifer, 40565 Encanto Way, Fremont, CA 94539, US,
TRIMBERGER Stephen M, 1261 Chateau Drive, San Jose, CA 95120, US,
THENDEAN John M, 1435 Martin Luther King Jr. Way #5, Berkeley, CA 94709, US,
RAO Kameswara K, 1172 Arlington Lane, San Jose, CA 95129, US,
Legal Representative:
CHANROO Keith A (et al) (agent), Xilinx, Inc., 2100 Logic Drive, San Jose, CA 95124, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200244876 A2-A3 20020606 (WO 0244876)
Application: WO 2001US45056 ~~20011128~~ (PCT/WO US0145056)
Priority Application: US 2000724652 20001128
Designated States: CA JP
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
Main International Patent Class: G06F-001/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 13434

English Abstract
To prevent copying of a design implemented in a **programmable logic device** (**PLD**), the **PLD** itself stores a decryption key or keys loaded by the designer, and includes a decryptor for decrypting an encrypted configuration bitstream as it is loaded into the **PLD** . The **PLD** also includes logic for reading header information that indicates whether the bitstream is encrypted, and can accept both encrypted and unencrypted bitstreams. The **encryption keys** may be **stored** in non-volatile memory or backed up with a battery so that they are retained when power is removed.

French Abstract
L'invention concerne un procede permettant d'empecher de copier une conception implantee dans une unite logique programmable (ULP), selon lequel l'ULP elle-meme stocke une ou plusieurs cles de decryptage chargees par le concepteur, et comprend un decrypteur servant a decrypter un flux binaire de configuration crypte alors qu'il est charge dans l'ULP. Cette derniere comprend egalement une logique servant a lire des informations d'en-tete indiquant si le flux binaire est crypte, et peut accepter des flux binaires cryptes et non cryptes. Les cles de cryptage peuvent etre stockees dans une memoire non volatile ou sauvegardees au moyen d'une batterie, de facon a etre conservees lorsque l'alimentation

est coupee.

Legal Status (Type, Date, Text)
Publication 20020606 A2 Without international search report and to be republished upon receipt of that report.
Examination 20021017 Request for preliminary examination prior to end of 19th month from priority date
Search Rpt 20030912 Late publication of international search report
Republication 20030912 A3 With international search report.

Fulltext Availability:
Detailed Description

English Abstract
To prevent copying of a design implemented in a **programmable logic device** (**PLD**), the **PLD** itself stores a decryption key or keys loaded by the designer, and includes a decryptor for decrypting an encrypted configuration bitstream as it is loaded into the **PLD** . The **PLD** also includes logic for reading header information that indicates whether the bitstream is encrypted, and can accept both encrypted and unencrypted bitstreams. The **encryption keys** may be **stored** in non-volatile memory or backed up with a battery so that they are retained when power ...

Detailed Description
... determine the value of the key. The well-known Data Encryption Standard DES used a 56-bit **encryption key** , and has been'broken in a few hours by a sophisticated computer to reveal the key. DES...

...resides in the key. When the encryption method is symmetrical, the same keys used for encryption are **stored** in the **PLD** and used in reverse order for decryption.

In a PLD offering multiple keys, if the number of...

11/5,K/9 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00910751 **Image available**
PROGRAMMABLE LOGIC DEVICE WITH METHOD OF PREVENTING READBACK
UNITE LOGIQUE PROGRAMMABLE ET PROCEDE EMPECHANT LES RECOPIES
Patent Applicant/Assignee:
XILINX INC, 2100 Logic Drive, San Jose, CA 95124, US, US (Residence), US (Nationality)
Inventor(s):
PANG Raymond C, 1138 Falcon Ridge Court, San Jose, CA 95120, US,
SZE Walter N, 20439 Kirkmont Drive, Saratoga, CA 95070, US,
THENDEAN John M, 1435 Martin Luther King Jr. Way #5, Berkeley, CA 94709, US,
TRIMBERGER Stephen M, 1261 Chateau Drive, San Jose, CA 95120, US,
WONG Jennifer, 40565 Encanto Way, Fremont, CA 94539, US,
Legal Representative:
CHANROO Keith A (et al) (agent), Xilinx, Inc., 2100 Logic Drive, San Jose, CA 95124, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200244875 A2-A3 20020606 (WO 0244875)
Application: WO 2001US45055 20011128 (PCT/WO US0145055)
Priority Application: US 2000724975 20001128
Designated States: CA JP
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
Main International Patent Class: G06F-001/00
Publication Language: English
Filing Language: English

Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 13249

English Abstract
It is sometimes desirable to protect a design used in a PLD from being copied. If the design is stored in a diferent device from the PLD and read into the PLD through a bitstream, the design may be encrypted as it is read into the PLD and decrypted within the PLD before being loaded into configuration memory cells for configuring the PLD. According to the invention, in such a device, a method is provided to prevent the design from being read back from the PLD in its decrypted state if it had been encrypted when loaded into the PLD.

French Abstract
Il est parfois souhaitable de proteger une conception utilisee dans une ULP (unite logique programmable) contre les copies. Si la conception est stockee dans un dispositif different de l'ULP et memorisee dans l'ULP a travers un flux binaire, la conception peut etre cryptee alors qu'elle est memorisee dans l'ULP et decryptee a l'interieur de cette derniere avant d'etre chargee dans des cellules de memoire de configuration pour configurer l'ULP. L'invention concerne un procede permettant d'empecher que la conception soit recopiee de l'ULP dans son etat decrypte si elle a ete cryptee lors de son chargement dans l'ULP.

Legal Status (Type, Date, Text)
Publication 20020606 A2 Without international search report and to be republished upon receipt of that report.
Examination 20021017 Request for preliminary examination prior to end of 19th month from priority date
Search Rpt 20030912 Late publication of international search report
Republication 20030912 A3 With international search report.

Fulltext Availability:
Detailed Description

Detailed Description
... rather than using nonvolatile memory to preserve keys, the invention preferably uses a battery connected to the **PLD** to preserve the key when power is removed from the **PLD** . Whereas it is possible to remove a **PLD** storing keys in nonvolatile memory, decap the **PLD** and observe
3
which of the nonvolatile bits are programmed to logic 1 ...logic 0, it is believed that it is very difficult to detern-dne the contents of keys **stored** only in static memory cells since power must be maintained to the memory cells storing the keys in order for the keys to even
be **stored** , and the **PLD** would have to be decapped, delayered, and probed
while operating power is continuous to the **PLD** . ,
W!qys an attacker can steal a desigLi once loaded into a **PLD**
If a key does not offer sufficient security,, an attacker may break the encryption code and determine the value of the key. The well-known Data Encryption Standard DES used a 56-bit **encryption key** , and has been broken in a few hours by a sophisticated computer to reveal the key. DES ...

...resides in the
key. When the encryption method is symmetrical, the same keys used for encryption are **stored** in the **PLD** and used in reverse order for decryption.

In a PLD offering multiple keys, if the number of...

11/5,K/10 (Item 7 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00876811 **Image available**

SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR DEVICE, OPERATING SYSTEM, AND NETWORK TRANSPORT NEUTRAL SECURE INTERACTIVE MULTI-MEDIA MESSAGING

SYSTEME, PROCEDE ET PRODUIT PROGRAMME D'ORDINATEUR POUR APPAREIL, SYSTEME D'EXPLOITATION ET MESSAGERIE MULTIMEDIA INTERACTIVE RESEAU, NEUTRE ET SECURISEE

Patent Applicant/Assignee:
STORYMAIL INC, 15729 Los Gatos Boulevard, Los Gatos, CA 95032, US, US (Residence), US (Nationality)
Inventor(s):
ILLOWSKY Daniel H, 21363 Dexter, Cuptertino, CA 95014, US,
WENOCUR Michael L, 4057 Amaranta Avenue, Palo Alto, CA 94306, US,
BALDWIN Robert W, 990 Amarillo Avenue, Palo Alto, CA 94303, US,
SAXBY David B, 14946 Granite Court, Saratoga, CA 95070, US,
Legal Representative:
ANANIAN R Michael (et al) (agent), Flehr Hohbach Test Albritton & Herbert LLP, 4 Embarcadero Center, Suite 3400, San Francisco, CA 94111-4187, US
,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200210962 A1 20020207 (WO 0210962)
Application: WO 2001US23713 20010727 (PCT/WO US0123713)
Priority Application: US 2000627357 20000728; US 2000627358 20000728; US 2000627645 20000728; US 2000628205 20000728; US 2000706606 20001104; US 2000706609 20001104; US 2000706610 20001104; US 2000706611 20001104; US 2000706612 20001104; US 2000706613 20001104; US 2000706614 20001104; US 2000706615 20001104; US 2000706616 20001104; US 2000706617 20001104; US 2000706621 20001104; US 2000706661 20001104; US 2000706664 20001104; US 2001271455 20010225; US 2001912715 20010725; US 2001912936 20010725; US 2001912905 20010725; US 2001912773 20010725; US 2001912885 20010725; US 2001912860 20010725; US 2001912941 20010725; US 2001912901 20010725; US 2001912772 20010725
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-017/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 169299

English Abstract
System, method, signal, operating model, and computer program for electronic messaging. Systems and method for providing security for communication of electronic messages, interactive sessions, software downloads, software upgrades, and other content from a source to a receiving device as well as signals used for such communications (304, 309, 308, 324, 342, 338, 334, 330, 326). Systems, methods, signals, device architectures, data formats, and computer program structures for providing authentication, integrity, confidentiality, non-repudiation, replay protection, and other security properties while minimizing the network (306) bandwidth, computational resources and manual user interactions (314) required to install, enable, deploy and utilize these security properties. System, device, method, computer program, and computer program product for searching and slecting data and control elements in message procedural/data sets for automatic and complete portrayal of message to maintain message intent.

French Abstract
Systeme, procede, signal, modele operatoire et programme d'ordinateur pour messagerie electronique. Systemes et procede permettant de securiser la communication de donnees de messages electroniques, sessions interactives, telechargements de logiciels, mises a jour de logiciels et autres contenus d'une source a un appareil recepteur ; signaux utilises pour ce type de communication (304, 309, 308, 324, 342, 338, 334, 330, 326). Systemes, procedes, signaux, architectures d'appareils, formats de donnees et structures de programmes d'ordinateur assurant l'authentification, l'integrite, la confidentialite, la non-repudiation, la protection contre la reinsertion ainsi que d'autres proprietes de securite tout en reduisant la bande passante du reseau (306), ressources informatiques et interactions manuelles de l'utilisateur (314) requises pour l'installation, l'activation, le deploiement et l'utilisation de ces proprietes de securite. Systeme, appareil, procede, programme d'ordinateur et produit programme d'ordinateur permettant de rechercher et de selectionner des elements de donnee et de commande dans des procedures relatives aux messages et des ensembles de donnees pour obtenir une representation automatique et complete du message et preserver l'intention du message.

Legal Status (Type, Date, Text)
Publication 20020207 A1 With international search report.
Publication 20020207 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20030116 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... with a trusted public key) or cryptographic checksum (verified with a trusted key derived from a Master **Key** or Session Key or Message Key).

For example, the trusted storage means can be data from a...

...which -case, -the-Mercha@nt-will'auth-enticate*the Clientbased on this Resource Tag. The Client's **keys** and certificate chain can be unique to this client, and the Merchant can authenticate the Client using...the Client based on this Resource Tag. (261) The method in embodiment (252), wherein the Client's **keys** and certificate chain are unique to this client, and the Entity authenticates the Client using this unique...

11/5,K/11 (Item 8 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00774564 **Image available**
INTERNET PAYMENT, AUTHENTICATION AND LOADING SYSTEM USING VIRTUAL SMART CARD
SYSTEME DE PAIEMENT, D'AUTHENTIFICATION ET DE CHARGEMENT PAR INTERNET AU MOYEN D'UNE CARTE A PUCE VIRTUELLE
Patent Applicant/Assignee:
VISA INTERNATIONAL SERVICE ASSOCIATION, 900 Metro Center Boulevard, Foster City, CA 94404, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
DAVIS Virgil M, 1121 Runnymead Drive, Los Altos, CA 94024, US, US (Residence), US (Nationality), (Designated only for: US)
CUTINO Suzanne C, 431 Arkansas Street, San Francisco, CA 94107, US, US (Residence), US (Nationality), (Designated only for: US)
REID Margaret, 970 Chestnut Street, #11, San Francisco, CA 94109, US, US (Residence), GB (Nationality), (Designated only for: US)

HOFFMAN Steve R, 293 Trenton Circle, Pleasanton, CA 94566, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
WEAVER Jeffrey K, Beyer Weaver & Thomas, LLP, P.O. Box 130, Mountain View, CA 94042-0130, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200108113 A1 20010201 (WO 0108113)
Application: WO 2000US19984 20000721 (PCT/WO US0019984)
Priority Application: US 99359083 19990722
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G07F-019/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 23634

English Abstract
A system (250) loads, authenticates and uses a virtual smart card for payment of goods and/or services purchased on-line over the Internet. An online purchase and load (OPAL) server (260) includes a virtual smart card data base (270) that has a record of information for each smart card that it represents for a user at the behest of an issuer. The server includes a smart card emulator (266) that emulates a smart card by using the card data base and a hardware security module (268). The emulator interacts with a pseudo card reader module (264) in the server that imitates a physical card reader. The server (260) also includes a client code module (224) that interacts with the pseudo card reader and a remote payment (206) or load server (862). A pass-through client terminal (204) presents a user interface and passes information between the OPAL server and a merchant server (208), and between the OPAL server and a bank server (860). The Internet (202) provides the routing functionality between the client terminal and the various servers. A merchant advertises goods on a web site (208). A user uses the client terminal (204) to purchase goods and/or services from the remote merchant server (208). The payment server (206) processes, confirms and replies to the merchant server. The payment server is also used to authenticate (206') the holder of a virtual card who wishes to redeem loyalty points from a merchant. To load value, the client terminal requests a load from a user account at the bank server (860). The load server (862) processes, confirms and replies to the bank server.

French Abstract
L'invention concerne un systeme (250) qui permet de charger, d'authentifier et d'utiliser une carte a puce virtuelle pour le paiement de biens et/ou de services achetes en ligne par le biais d'Internet. Un serveur (260) d'achat et de chargement en ligne (OPAL) comprend notamment une base de donnees de cartes a puce virtuelles (270) qui stocke des informations relatives a chaque carte a puce virtuelle qu'elle represente pour un utilisateur a la demande d'un emetteur. Le serveur comprend un emulateur de carte a puce (266) qui emule une carte a puce au moyen de la base de donnees de cartes et un module de securite du materiel (268). L'emulateur interagit avec un pseudo module de lecteur de cartes (264) qui imite, dans le serveur, un lecteur de cartes physique. Le serveur (260) comprend egalement un module de code client (224) qui interagit avec le pseudo lecteur de cartes et un serveur de paiement (206) ou de chargement (862) a distance. Un terminal client (204) presente une interface utilisateur et fait passer les informations entre le serveur OPAL et le serveur commercial (208), et entre le serveur OPAL et un

serveur bancaire (860). L'Internet (202) assure les fonctions d'acheminement entre le terminal client et les differents serveurs. Le commercant fait connaitre ses produits sur un site web (208). Le consommateur utilise le terminal client (204) pour acheter des biens et/ou des services aupres du serveur commercial a distance (208). Le serveur de paiement (206), apres traitement, confirme et repond au serveur commercial. Le serveur de paiement sert egalement a authentifier (206') le detenteur d'une carte virtuelle qui desire encaisser des points de fidelite aupres du commercant. Pour charger la valeur, le terminal client demande un chargement a partir d'un compte utilisateur aupres du serveur bancaire (860). Le serveur de chargement (862), apres traitement, confirme et repond au serveur bancaire.

Legal Status (Type, Date, Text)

Publication	20010201	A1 With international search report.
Publication	20010201	A1 Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.
Examination	20010726	Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Claims

Claim
... generating a virtual card signature S3 may still occur. In the alternative embodiment in which points are **stored** in card data base 270, the points needed to redeem the benefit chosen by the consumer from ...

...access to a privileged service for the benefit requested. In the alternative embodiment in which points are **stored** in card data base 270, the Authentication Result message serves not only as an authentication of the...implemented as a security card described above or similar to HSM 268 above. HSM 864 contains the **encryption keys** used for generating signatures (for example S 1, S2 and S3) that provide security for the transaction...and, in general, to provide for a valid transaction and to prevent fraud. HSM 268 also includes **encryption keys** for the generation of a virtual card signature. In an alternative embodiment, HSM 864 could be replaced...

...that includes a security card such as is shown in the previous embodiments. In this situation, the **encryption keys** would be **stored** in the security card. Briefly, system 850 operates as follows. A consumer accesses bank server 860 using...of subsystems. Processor(s) 922 (also referred to as central processing units, or CPUs) are coupled to **storage** devices including
memory 924. Memory 924 includes random access memory (RAM) and read-only memory (ROM). As...

...below. A fixed disk 926 is also coupled bi-directionally to CPU 922; it provides additional data **storage** capacity and may also include any of the computer-readable media described below. Fixed disk 926 may be used to store programs, data and the like and is typically a secondary **storage** medium (such as a hard disk) that is slower than primary **storage** . It will be appreciated that the information retained within fixed disk 926, may, in appropriate cases, be...shares a portion of the processing. In addition, embodiments of the present invention further relate to computer **storage** products with a computer-readable medium that have computer code thereon for performing various computer-implemented operations...

...that are specially configured to store and execute program code, such as application-specific integrated circuits (ASICs), **programmable logic devices** (PLDs) and ROM and RAM devices. Examples of
computer code include machine code, such as pr

oduced...

11/5,K/12 (Item 9 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00736251 **Image available**
COMMAND CONSOLE FOR HOME MONITORING SYSTEM
CONSOLE DE COMMANDE POUR SYSTEME DOMOTIQUE
Patent Applicant/Assignee:
EARLY WARNING CORPORATION, P.O. Box 4476, Wheaton, IL 60189-4476, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
QUIGLEY Mark P, 3S440 Herrick Road, Warrenville, IL 60555, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
PENN Amir N, McDonnell Boehnen Hulbert & Berghoff, 32nd floor, 300 South Wacker Drive, Chicago, IL 60606, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200049589 A1 20000824 (WO 0049589)
Application: WO 2000US4568 20000222 (PCT/WO US0004568)
Priority Application: US 99255421 19990222
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G08B-019/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 91331

English Abstract
A method and apparatus for a home monitoring system is provided. The home monitoring system may include a command console (10) for monitoring and processing the output of sensors (14, 16, 18, 20, 22, 24). The processing of the sensors (14, 16, 18, 20, 22, 24) includes (1) providing a history of the sensor as an indicator to the operator of the sensor output over time; (2) analyzing the trends of the sensor to increase the effectiveness of the sensor beyond simply the current sensor output; and (3) analyzing the output of one sensor which may impact interpretation of a second sensor's output. The monitoring system may also be a prescription reminder system. The prescription reminder system may be used in homes or institutional medical facilities (assisted living or nursing homes) to provide patients with a manner to remind them to take pharmaceutical drugs at prescribed times.

French Abstract
Il s'agit d'un procede et d'un dispositif utilises pour un systeme domotique. Ce systeme domotique peut comprendre une console de commande (10) pour controler et traiter les sorties de capteurs (14, 16, 18 20, 22, 24). Le traitement des capteurs (14, 16, 18, 20, 22, 24) vise a (1) fournir un historique du capteur qui servira d'indicateur a l'operateur sur les sorties du capteur au fil du temps; (2) analyser les tendances du capteur pour ameliorer son efficacite au-dela des seules sorties du capteur courant; et (3) analyser les sorties d'un capteur susceptibles d'avoir une incidence sur l'interpretation des sorties d'un deuxieme capteur. Le systeme de surveillance peut egalement servir d'aide-memoire pharmaceutique. Cet aide-memoire pharmaceutique peut etre utilise dans

des centres ou des etablissements de soins (maisons de retraite ou maisons de repos) et servir aux patients pour les avertir aux heures prescrites de prise des medicaments

Legal Status (Type, Date, Text)
Publication 20000824 A1 With international search report.
Examination 20010412 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Claims

Claim
... t'n.-s menu, which is to ARM or DISARM the nurgiar alarm. If ARMED then the **next** state will be to set if the burglar is to **determine** whether the alarm is HOME or AWAY. Each burglar sensor wi--" be either a HOME or a...

...burglar disabled, then if user is MASTER, then goto system configuration; otherwise goto main loop (monitor).
return: **next** main menu state
unsigned int BurglarAlarm (void
LCDcls
LCDprintf MsgTable MSG
BURGLAR-ALARM
1
LCDprintf MsgTable MSG...
...return (MAX-UserMenuSize
I /* end switch(cUserMode)
This module is part of the main menuing system. This **determines** if the
burglar sensor alarming is set for HOME or AWAY. See the ARM and DISARM routines for more details. **Next** state is Either configuration for MASTER or main loop for anyone else.
return: **next** main menu state
unsigned int BurglarAlarmHA (void
LCDcls /* Burglar system HOME/AWAY?
LCDprintf MsgTable MSG
BURGLAR
ALARM...

...flag
GetKey KeyMENU /* ACK
break
case KeyMENU:
break ; /* do nothing here
/* end of switch(cKeyValue)
switch (cUserMode) /* **determine** **next** state
case GOD:
return (CONFIG-SYS /* if god, goto conf system
default:
cUserMode = MONITOR MODE
; /* anyth4na else...

...of the area before the system will active the alarm and consider that person a burglar
return: **next** configuration menu state
unsigned int BurglarTimeout (void
if BurglarCount 0
if bBurglarTO BURGLAR-90SEC
LCDcls /* tell user...

...break ;
/* end switch(cKeyValue)
/* end if(bBurglarTO BURGLAR-45SEC
/* end if(BurglarCount 0
return MENU-BURGLARSO /* return **next** state

```
/* change to burglar timeout of 45 seconds
void Burglar45Sec ( void
bBurglarTO BURGLAR-45SEC ; /* set flag
LCDcls...
...user whether to turn the noisy stuff feature on or off, then set a bit
variable to indicate such. --his subroutine is executed as a state from
the menu-s state machine. It does not...final number. If an invalid call
 forwarding number is in the system X's are shown
 return: next configuration state
unsigned int CallForward ( void
unsigned char i
TestInitCallF ( ) ; /- check call forwarding number
LCDcls ( ) ; /* ask user...

...temp to current C.F.
uspdirty = 1 ; /* flag to write flash
newcfn 1
break
case KeyNO:
/* return next state to end, reenter Call Forward Number
return ( MENUCALL-FORWARD
case KeyMENU:
LCDcls ( ) ; /* they canceled, so keep...

...KeYMENU ) ; /* ack */
case KeyMENU: /* do nothing, cancel
break ;
/* end of switch(cKeyValue)
return ( MENU-TEST-LOCAL return next state
 This routine will take the temporary call forwarding array, which has
been copied from the current...

...count
for count = 0 count < LIMIT-CALLFORWARD count@+
user-space.us cfwd count Ox30
uspdirty
 This routine determines if the call forwarding number is valid, if it
is
 valid then the routine will call a...

...Flow of the menus can be changed very easily with changing enumeration
and *changing a pointer to next menu structure.
#include "gen
def.h"
unsigned int ( *fptrCFG [ MAX
ConfigStates I void
static unsigned int cConfigState...whether we want tone/pulse, etc. This
state mac'@-,ne works by passing the address of the next , function to
call, then simply using
 that address as a pointer call prototyped function
 return: next state of Menu system
unsigned in7 ConfigMENU void
cConfigState = 0 ini r4 a-, s-ate
while...

...of the configuration menu and will configure whether yqu are connected
to the NCSC or not.
 return: Next configuration state
unsigned int ConnectOptions ( void
 go to either Reconnect or Disconnect
 the default is DISCONNECTED from...

...KeyYES:
Disconnect /* Disconnect NCSC service
break
/* end if(user
space.us-flg & USFDISC)
```

```
return ( MENU-SW-VER /*  next  state
/* this will disconnect the Command consoi-e from the NCSC
void Disconnect ( void
user-space.us...

...Ox39 ) ;
GetKey KeyMENU /* wait for ACK
 This routine is part of the configuration Menuing system and will
determine   if the modem will dial direct or it will dial 9 before
dialing the number.
 return:  next  configuration menu state
unsigned int DialType( void
if rdosl 0
LCDcls display Direct diall set
LCDprintf MsgTable...Press Each Key /* MSG-TEST-LOCAL-6B
(11 Set Date? /* MSG
DATE
P Registration /* MSG- REG
i" Succeeded  <MENU>"), /* MSG-  SUCCEED
P Sound On <Y> MSG SOUND ON'Y
P Sound Off <N> /* MSG SOUND OFF N
Silent...

...DIAL-9,
MSG-DIAL-DIRECT,
MSG PROMPT,
MSG-ADD
SENSOR,
MSG-POSITTON
SENSOR,
MSG-TEST-SENSOR,
MSG- MORE -SENSORS,
MSG-SENSOR-ADDED,
MSG-SENSOR-NOT-ADDED,
MSG-SENSOR-ARRAY-FULL,
MSG-CANNOT-ADD-ANYMORE-SENSORS...

...MSG-TEST-LOCAL-5A,
MSG-TEST-LOCAL-5B,
MSG-TEST-LOCAL-6B,
MSG-DATE,
MSG-REG,
MSG- SUCCEED ,
MSG-SOUND-ON-Y,
MSG-SOUND-OFF-N,
MSG-SILENT-ON-Y,
MSG-SILENT-OFF-N,
MSG...

...IS DISCONNECTED
THESE EQUATES DEFINE THE FLAG BITS IN THE SENSOR ARRAY FLAGS FIELD.
THE PRESENT BIT  INDICATES  THAT THIS SENSOR ENTRY IN IN USE. IT IS
SET BY THE ADD SENSOR MENU WHEN A...

...SNFPRES EQU 01H 1 IF SENSOR PRESENT
; THIS BIT IS SET BY THE RF RECEIVE HANDLER TO  INDICATE  THAT A MESSAGE
WAS
; RECEIVED FROM THIS SENSOR. IT IS CLEARED BY VARIOUS ROUTINE WHICH
; POST PROCESS...S FOR THE LOW BATTERY CONDITION. IT IS CLEARED
BY MONITOR WHEN A MESSAGE IS RECEIVED THAT  INDICATES  THE BATTERIES
ARE OK.
SNFLBA EQU 80H 1 IF LOW BAT MSG ACK-D
; THESE BIT ARE...

...FORMAT OF A SENSOR STRUC. THIS IS ACTUALLY A SUBSTRUC OF
THE USER SPACE. IT CONTAINS SESNOR  SPECIFIC  INFORMATION. MAXSENSORS
DEFINES THE NUMBER OF THESE STRUCS. THERE MUST BE AT LEAST ONE FOR EACH
```

```
  SENSOR...
...1 DATA2 BYTE
  SEN-STAT EQU SEN-DATA2+1 STATUS BYTE
  SEN-NUHR EQU SEN-STAT+1  NEXT  UPDATE TIME HR:
  SEN-NUMIN EQU SEN-NUHR+1  NEXT  UPDATE TIME :MIN
  SEN-FLG2 EQU SEN-NUMIN+1 ANOTHER FLAGS BYTE
  SENSTRUCL EQU SEN-FLG2+1...WRITE LOOP
  PRLINE2: ;
  MOV i-0,#32
  PRLINELP:
  PUSH ARO SAVE LOOP CNT
  MOVX A,@DPTR GET  NEXT  CHAR TO WRITE
  INC DPTR BUMP BUFFER PTR
  PUSH DPL SAVE PTR
  PUSH DPH
  MOV R7,A...

...TO CALL THE NCSC.
  MOV B,#SS-KEYGET READ THE KEYBOARD
  LCALL SYSSVC
  MOV A,R6 GET  KEY   BITS  THAT COUNT
  JB ACC.7tIDKYMENU JUMP IF MENU KEY PRESSED
  ANL A,#70H MASK ALARM KEYS
  iz...LOW 500
  MOV B,#SS-DELAY
  LCALL syssvC
  POP ACC GET MASK BIT
  RL A SHIFT TO  NEXT  BIT
  MOV R7,A
  POP ARO GET LOOP COUNT
  DJNZ RO,REDlLP LOOP
  MOV B,#SS-LCDCLS...

...LOW 500
  MOV B,#SS-DELAY
  LCALL SYSSVC
  POP ACC GET MASK BIT
  RL A SHIFT TO  NEXT  BIT
  MOV R7,A
  POP ARO GET LOOP COUNT
  DJNZ RO,GRNlLP LOOP
  MOV B,#SS-LCDCLS...

...TREAT AS NOT PRESENT
  INC RO YES DUMP BURGLAR COUNT
  BANOTP: ;
  MOV A,DPL BUMP DPTR 'O  NEXT  SENSOR ENTRY
  ADD A,#LO7; (SENSTRUCL-1) ACCO',= 7OR THE !NC OF DPTR
  Mov DPL, A
  MOV...AN XOR OF ALL DATA FROM STX THRU ETX.
  THE INTERFACE TO THIS ROUTINE IS VIA THE  FOLLOWING  SUBROUTINES AND
  DATA AREAS. FIRST, THERE IS SOME P

  UBLIC FIXED DATA SPACE IN XRAM.
  IOOBUF THIS...KEY WAS PRESSED
  EV-KEYMENU: ;
  mov B,#SS-KEYGET READ THE KEYBOARD
  LCALL SYSSVC
  mov AoR6 GET  KEY   BITS  THAT COUNT
  mov C,ACC.7 GET THE MENU  KEY   BIT
  RET
  RETURN TRUE IF THE SENSOR ARRAY INDEX IS AT THE LAST SENSOR.
  EV-LASTSENS: ;
  CLR C...NEWCONN CLEAR THE CONNECT/DISCONNECT CHGD
  NOW LOOOP THRU ALL SENSOR ENTRIES CLEARING THOSE FLAG BITS WHICH
   INDICATE  A CONFIGURASTION CHANGE.
  MOV DPH,#HIGH USER-SPACE+US-SNS+SEN-FLAGS ; POINT TO 1ST SENSOR
```

MOV...

...LCD
AC-LCDM1: ;
mov R7,#'F' TELL SUBR TO PRINT FAILED MSG
CALL -PRREGMSG
RET
DISPLAY REGISTRATION **SUCCEEDED** MESSAGE ON THE LCD
AC-LCDM2: ;
mov R7,#'S' TELL SUBR TO PRINT FAILED MSG
CALL -PRREGMSG...

...THIS WILL CAUSE THE BOOT ROM CODE TO ASK FOR A DLL
OF THE APPLICATION AFTER THE **NEXT** RESET.
mov DPTR,#CLOBBER GET DATA TO CLOBBER WITH
mov DPH1,#HIGH BASEAPPL GET 1ST BYTE OF...OF THE USER SPACE. THIS WILL
CAUSE THE DEFAULT USER SPACE VALUES TO
BE LOADED AFTER THE **NEXT** RESET.
MOV DPTR,#CLOBBER GET SOME GARBAGE DATA
MOV DPH1,#HIGH FLASH SPACE+US SENT
; GET FLASH...
...simp s LOOP '@'NTIL DOG BARKS
ACRSPRET:
RET BACK TO CALLER
SET THE ALARM CALL BIT WHICH **INDICATES** WE MUST INFINITELY ATTEMPT
TO MAKE THE CALL UNTIL WE GET THRU.
AC
SETALC: ;
SETB ALCALL
RET...

...MARK USER SPACE DIRTY
RET
THIS ACTION SAVES THE CURRENT TIME IN RPINTIME TO BE USED TO **DETERMINE**
WHEN WE MUST **NEXT** REPORT IN TO THE NCSC. IF THE SYSTEM IS CONFIGURED
FOR MONTHLY CHECKIN, THE CURRENT MONTH & DAY...

...FOR MONTHLY CHECKIN THE DAY
IS TRUNCATED TO THE 28TH. THIS IS BECAUSE THE CHECKIN TIME IS **DETERMINED**

CHECKING THAT THE RPINTIME MONTH & CURRENT MONTH ARE DIFFERENT, BUT THAT
THE DAY IS THE SAME. THIS...
...SOME
MONTHS DONT HAVE MORE THAN 28 DAYS. IF RPINTIME IS SET TO THE 31ST, AND
THE **NEXT** MONTH DOESNT HAVE 31 DAYS, THERE WILL BE NO CHECKIN UNTIL A
MONTH
THAT HAS 31 DAYS...R M
THE PURPOSE OF THIS SUBROUTINE IS TO COMPOSE THE COMMON FIELDS
OF THE SEVERAL SENSOR **SPECIFIC** MESSAGES. WE WILL PUT THE SENSOR
ARRAY INDEX, SENSOR TYPE & SERIAL NUMBER INTO THE NCSC MSG BUFFER...

...prompt for the user to enter a PIN number in the system and then call
ReadPINStruct to **determine** if they entered the correct pin or not. If
they did, they will be let into the...

...is called from the MainPIN routine, this will read the PIN the user
has entered, and then **determine** what access they have, if any. IT does
this by setting the cUserMode, which can be set...

11/5,K/13 (Item 10 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00731954 **Image available**
AUTOMATED INFORMATION FILTERING AND DISTRIBUTION SYSTEM
SYSTEME AUTOMATISE DE DISTRIBUTION ET DE FILTRAGE DE L'INFORMATION

Patent Applicant/Assignee:
ENUNTIO INC, 779-E East Evelyn Avenue, Sunnyvale, CA 94041, US, US (Residence), US (Nationality)
Inventor(s):
KANODIA Rajendra Kumar, 3717 Ortega Court, Palo Alto, CA 94303, US
BLACK Steven Todd, 412 O'Keefe Street, Menlo Park, CA 94025, US
Legal Representative:
MARINO Fabio E, Skjerven, Morrill, MacPherson, Franklin & Friel LLP, Suite 700, 25 Metro Drive, San Jose, CA 95110, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200045285 A1 20000803 (WO 0045285)
Application: WO 2000US404 20000107 (PCT/WO US0000404)
Priority Application: US 99229393 19990111
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-015/16
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 9219

English Abstract
An efficient and scalable real-time information distribution system and method of operation thereof are provided that build customized information collections according to individual preferences. This distribution system uses an information distribution network (130) such as the Internet for its communications infrastructure. Scalability and efficiency is realized by routing information through the information distribution network (130). Information streams enter the information distribution network through feed processors (110A-110B). Feed processors (110A-110B), in turn, parse the information received from feed sources (120A-120B) and create a set of "keyples." The keyples are then passed on to a series of keyple routers (160A-160D). The keyple routers match the keyples to a set of destinations, thus multiplexing the keyples to only those destinations that have requested the information. A destination can consist of either another keyple router or a keyple customizer which assigns keyples to collections and then passes them on to a collection builder which constructs custom keyple collections for individual users (150).

French Abstract
Cette invention concerne un systeme efficace de distribution de l'information, evolutif, en temps reel, et sa methode d'exploitation qui permettent de creer des ensembles d'informations personnalises en fonction de preferences individuelles. Ce systeme de distribution repose sur un reseau de distribution de l'information tel qu'Internet pour son infrastructure de communications. Le systeme selon l'invention peut atteindre un degre eleve d'evolutivite et d'efficacite en acheminant l'information via le reseau de distribution de l'information (130). Les trains d'information penetrent dans le reseau de distribution (130) par des processeurs d'alimentation (110A-110B). Ces processeurs (110A-110B) analysent l'information recue des sources d'alimentation (120A-120B) et creent des jeux de fichiers de cle (keyples). Ces fichiers de cle sont ensuite transferes sur une serie de routeurs (160A-160D). Ces routeurs preparent les fichiers de cles en fonction d'une serie de destinations, en les multiplexant uniquement que vers les destinations qui demandent l'information. Une destination peut se presenter sous la forme soit d'un autre routeur de fichier de cles ou d'un dispositif de personnalisation de fichiers de cles. Ce dispositif de personnalisation attribue les

fichiers de cle entrants a des collections, puis a un dispositif de realisation de collection. Un dispositif de realisation de collection cree a son tour des fichiers de cles personnalises pour des utilisateurs individuels (150).

Legal Status (Type, Date, Text)
Publication 20000803 A1 With international search report.
Publication 20000803 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20001116 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Claims

Claim
... browser.
ISO/&)-SOB 15c)
TF
bytes rsion Number
4 bytes Feed ID
4 bytes essagelD yple
4 **bytes** **Key** ID (24 bytes)
4 bytes Even 2S.
4 bytes Timest
?A
2"70
4 bytes version Number...

...Customized
4 bytes eyple
4 bytes Bytes)
4 bytes
r2
In a
Memory
Block
The Version Number
indicates the version of the
Keyple being constructed.
Insert Version
Number
F-The Feed ID is a unique...

...L numberof messages
generated for a particular
Feed that match a particular
Key.
Insert EventCount
The Timestamp **indicates** the
time the message originated
in a standard format defined
by eNuntio.
Insert mes mp
2c
eyple Generated
essage
Each Message may have one or **more**
Keys assoCiated with it. In addition, a
Wildca rd Key may be active which
matches any Message from...Classification (IPC) or to both national classification and IPC
B. FIELDS SEARCHED
Minimum documentation searched (classification system **followed** by classification symbols)
U.S. : 709/225, 229

Documentation searched other than minimum documentation to the extent...

...practicable, search terms used)
WEST, IEEE
C. DOCUMENTS CONSIDERED TO BE RELEVANT
Category* Citation of document, with **indication** , where appropriate, of the relevant passages Relevant to claim No.
Y US 5,754,938 A (HERZ...

11/5,K/14 (Item 11 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00507977 **Image available**
METHOD AND APPARATUS FOR GENERATING MUSICAL EFFECTS
PROCEDE ET APPAREIL DE GENERATION D'EFFETS MUSICAUX
Patent Applicant/Assignee:
KAY Stephen,
Inventor(s):
KAY Stephen,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9939329 A1 19990805
Application: WO 99US1812 19990128 (PCT/WO US9901812)
Priority Application: US 9872918 19980128; US 9872919 19980128; US 9872921 19980128; US 9872922 19980128
Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Main International Patent Class: G10H-001/02
International Patent Class: G10H-001/26; G10H-001/30; G10H-001/40
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 91610

English Abstract
An initial note series (104) is collected from a real-time source of musical input material (101) such as a keyboard or a sequencer playing back musical data, or extracted from musical data stored in memory (122). The initial note series may be altered to create variations of the initial note series using various mathematical operations. The resulting altered note series (110), or other data stored in memory is read out according to one or more patterns (116). The patterns may have steps containing pools of independently selectable items from which random selections are made. A pseudo-random number generator (142) is employed to perform the random selections during processing, where the random sequences thereby generated have the ability to be repeated at specific musical intervals.

French Abstract
L'invention concerne la collecte d'une serie de notes initiales (104) a partir d'une source d'entree de matiere musicale (101) en temps reel telle qu'un clavier ou un sequenceur reproduisant des donnees musicales; ou alors l'extraction de cette serie de notes initiales de donnees musicales mises en memoire (122). On peut modifier la serie de notes initiales pour creer des variations sur les notes initiales grace a plusieurs operations mathematiques. La serie de notes modifiees obtenue (110) ou d'autres donnees mises en memoire sont lues en fonction d'une ou de plusieurs configurations (116). Les configurations peuvent comporter des phases comprenant des groupes d'articles pouvant etre selectionnes au hasard et a partir desquels on procede a des selections au hasard. On utilise un generateur de nombres pseudo-aleatoires (142) pour effectuer

Set	Items	Description
S1	679	ENCRYPTION()(KEY OR KEYS)
S2	642353	STORED OR BACKUP OR BACK()UP OR STORAGE
S3	13996	PLD OR PROGRAMMABLE()LOGIC()DEVICE?
S4	393	(KEY OR KEYS)(N)(BIT OR BITS OR BITE OR BITES OR BYTES)
S5	5838612	INDICAT? OR DETERMIN? OR SPECIF? OR SIGNIF?
S6	372	(MORE OR FURTHER OR ADDITIONAL)(N)(KEY OR KEYS)
S7	2101796	FOLLOW? OR SUCCEED? OR NEXT OR SUBSEQUENT?
S8	0	S1 AND S2 AND S3
S9	0	S4 AND S5 AND S6
S10	96	S1 AND S2
S11	80	S4 AND S5
S12	132	S5 AND S6
S13	5	S4 AND S6
S14	217	S11 OR S12 OR S13
S15	0	S1 AND S3
S16	20	S14 AND S7
S17	16	S16 NOT PY>2000
S18	16	S17 NOT PD>20001128RD

File 8:Ei Compendex(R) 1970-2004/May W4
(c) 2004 Elsevier Eng. Info. Inc.
File 35:Dissertation Abs Online 1861-2004/May
(c) 2004 ProQuest Info&Learning
File 202:Info. Sci. & Tech. Abs. 1966-2004/May 14
(c) 2004 EBSCO Publishing
File 65:Inside Conferences 1993-2004/May W5
(c) 2004 BLDSC all rts. reserv.
File 2:INSPEC 1969-2004/May W4
(c) 2004 Institution of Electrical Engineers
File 233:Internet & Personal Comp. Abs. 1981-2003/Sep
(c) 2003 EBSCO Pub.
File 94:JICST-EPlus 1985-2004/May W2
(c)2004 Japan Science and Tech Corp(JST)
File 99:Wilson Appl. Sci & Tech Abs 1983-2004/Apr
(c) 2004 The HW Wilson Co.
File 95:TEME-Technology & Management 1989-2004/May W2
(c) 2004 FIZ TECHNIK
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
(c) 2002 The Gale Group

18/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

01829328 E.I. Monthly No: EI8512114930 E.I. Yearly No: EI85027294
Title: ON THE POWER OF CASCADE CIPHERS.
Author: Even, S.; Goldreich, O.
Corporate Source: Technion-Israel Inst of Technology, Haifa, Isr
Source: ACM Trans Comput Syst v 3 n 2 May 1985 p 108-116
Publication Year: 1985
CODEN: ACSYEC
Language: ENGLISH
Document Type: JA; (Journal Article) Treatment: T; (Theoretical)
Journal Announcement: 8512
Abstract: The unicity distance of a cascade of random ciphers, with respect to known plaintext attack, is shown to be the sum of the key lengths. At time-space trade-off for the exhaustive cracking of a cascade of ciphers is shown. The structure of the set of permutations realized by a cascade is studied; it is shown that only l. 2**k exhaustive experiments are necessary to **determine** the behavior of a cascade of l stages, each having k **key bits** . It is concluded that the cascade of random ciphers is not a random cipher. Yet, it is shown that, with probability, the number of permutations realizable by a cascade of l random ciphers, each having k **key bits** , is 2**l**k. **Next** , it is shown that two stages are not worse than one, by a simple reduction of the cracking problem of any of the stages to the cracking problem of the cascade. Finally, it is shown that proving a nonpolynomial lower bound on the cracking problem of long cascades is a hard task, since such a bound implies that P NOT-EQUAL NP. (Author abstract) 7 refs.
Descriptors: *CRYPTOGRAPHY; DATA PROCESSING--Security of Data
Identifiers: CASCADE CIPHERS; DATA ENCRYPTION; RANDOM CIPHERS; UNICITY DISTANCE
Classification Codes:
723 (Computer Software)
72 (COMPUTERS & DATA PROCESSING)

18/5/2 (Item 1 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

01741010 ORDER NO: AADAA-I9968864
A visual study of acid-neutralizing ability of marine cylinder lubricants
Author: Wu, Rong Chang
Degree: Ph.D.
Year: 1999
Corporate Source/Institution: Tulane University (0235)
Chairman: Kyriakos D. Papadopoulos
Source: VOLUME 61/04-B OF DISSERTATION ABSTRACTS INTERNATIONAL. PAGE 2079. 130 PAGES
Descriptors: ENGINEERING, CHEMICAL ; ENGINEERING, MARINE AND OCEAN
Descriptor Codes: 0542; 0547

The combustion of high level sulfur-containing (2–5%) fuels generates sulfuric acid in marine diesel engines. In the absence of any control, sulfuric acid attacks metal surfaces and is the prime cause of ring and cylinder bore wear. One of the major requirements of the marine cylinder lubricant (MCL) is therefore their ability to neutralize the sulfuric acid and any other acids formed during the combustion process. The MCL's additives for acid neutralization are basically oil-soluble Group-II basic metal (calcium or magnesium) overbased sulfonates, or phenates. Those overbased detergents are in the form of reverse micelles with a calcium carbonate core, which is stabilized by an outer alkyl/aryl sulfonic acid shell.

In this study, a capillary video-microscopy technique was used to develop an experimental protocol for ranking the ability of marine cylinder

Encoding
Classification Codes and Description: 4.08 (Coding, Compacting); 6.06 (Life Sciences and Biomedicine)
Main Heading: Information Recognition and Description; Information Systems and Applications

18/5/9 (Item 2 from file: 202)
DIALOG(R)File 202:Info. Sci. & Tech. Abs.

2103794
Key-word retrieval electronic translator (Patent).
Author(s): Hashimoto, S; Morimoto, M.; Yamamoto, H.; Yanagiuichi, S.
Patent Number(s): US 4630235
Publication Date: Dec 16, 1986
Language: English
Document Type: Patent
Record Type: Abstract
Journal Announcement: 2100

An improved electronic translator wherein an arrangement of words in a source language is retrieved from a memory contained therein along with atranslation of said arrangement of words in a target language different from said source language, said translator comprising: Input means for serially entering two or **more key** words thought by a user to be contained within at least one stored arrangement of words in said source language; Memory means for storing a plurality of stored arrangements of words in said source language and an associated plurality of stored arrangement of words in said target language, each one of said plurality of stored arrangements of words in said source language being associated with its translation as a stored arrangement of words in said target language; Access means, responsive to said input means, for searching the plurality of stored arrangements of words in said source language to locate a word therein corresponding to a said key word; Termination means, responsive to the completed entry of each one of said two or **more key** words by said input means, for **indicating** that said entry of each said key word is completed and for immediately enabling said access means to search said plurality of stored arrangements of words to identify a word therein corresponding to said key word before a **succeeding** said key word is entered; Said access means, upon entry of two or **more key** words contained within said memory means as **determined** by the search of said access means enabled by said translation means, recalling from said memory means a said stored arrangement of words in said source language containing said two or **more key** words entered into said input means as a selected source arrangement and recalling its said translation as selected translation arrangement, and means, responsive to the recall of said selected source arrangement and said selected translation sentence by said access means, for **indicating** said selected source arrangement and said selected translation arrangement to the user of said translator.

Descriptors: Electronic information systems; Information retrieval; Keywords; Patents
Classification Codes and Description: 5.11 (Searching and Retrieval); 5.05 (Hardware)
Main Heading: Information Processing and Control

18/5/10 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

5865750 INSPEC Abstract Number: B9805-6120B-002, C9805-6130S-004
Title: DES is dead! Long live????
Author(s): Rothke, B.
Journal: Information Systems Security vol.7, no.1 p.57-60
Publisher: Auerbach Publications,

Publication Date: Spring 1998 Country of Publication: USA
CODEN: ISSEFH ISSN: 1065-898X
SICI: 1065-898X(199821)7:1L.57:DLL;1-E
Material Identity Number: F173-98002
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: The Data Encryption Standard (DES) is an encryption cipher defined and endorsed by the US government in 1977 as an official federal standard. DES has been extensively studied since its inception and is both the most well known and most widely used cryptosystem in the world. DES was intended to provide strong encryption for the government's sensitive but unclassified information. In December 1998, DES will be retired as a federal cryptographic standard. Its retirement is coming after more than 23 years of illustrious use. Being over 23 years old, DES is ancient in the world of computing. At the technical level, DES has a 64-bit block size and uses a 56- **bit key** during encryption. The National Institute for Standards and Technology (NIST) has recertified DES as an official US government encryption standard on numerous occasions. This recertification occurs every five years. DES was last recertified in 1993 and NIST has **indicated** that it will not recertify DES. For those companies that desire a common cryptographic encryption algorithm, the **next** few years will be difficult and strained. When DES was reaffirmed for the final time in 1993, the plans for its successor should have been at an advanced stage. It was reckless of NIST to wait until September 1997 to post the announcement for the AES in the Federal Register. This is a classic case of standards not keeping up with the times. Companies will now have to look at their security and cryptographic infrastructure and perform a serious risk analysis. (0 Refs)
Subfile: B C
Descriptors: code standards; cryptography; government data processing
Identifiers: Data Encryption Standard; DES encryption cipher; US government; official federal standard; unclassified information; federal cryptographic standard; official US government encryption standard; recertification; cryptographic encryption algorithm; NIST; AES; cryptographic infrastructure; risk analysis
Class Codes: B6120B (Codes); C6130S (Data security); C7130 (Public administration)

18/5/11 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

02608879 INSPEC Abstract Number: B86016124, C86014200
Title: On the power of cascade ciphers
Author(s): Even, S.; Goldreich, O.
Author Affiliation: Technion-Israel Inst. of Technol., Haifa, Israel
Journal: ACM Transactions on Computer Systems vol.3, no.2 p.108-16
Publication Date: May 1985 Country of Publication: USA
CODEN: ACSYEC ISSN: 0734-2071
U.S. Copyright Clearance Center Code: 0734-2071/85/0500-0108$00.75
Language: English Document Type: Journal Paper (JP)
Treatment: Theoretical (T)
Abstract: The unicity distance of a cascade of random ciphers, with respect to known plaintext attack, is shown to be the sum of the key lengths. A time-space trade-off for the exhaustive cracking of a cascade of ciphers is shown. The structure of the set of permutations realized by a cascade is studied; it is shown that only 1.2/sup k/ exhaustive experiments are necessary to **determine** the behavior of a cascade of 1 stages, each having k **key bits** . It is concluded that the cascade of random ciphers is not a random cipher. Yet, it is shown that, with high probability, the number of permutations realizable by a cascade of 1 random ciphers, each having k **key bits** , is 2/sup 1k/. **Next** , it is shown that two stages are not worse than one, by a simple reduction of the cracking problem of any of the stages to the cracking problem of the cascade. Finally, it is shown that proving a nonpolynomial lower bound on the cracking problem of

long cascades is a hard task, since such a bound implies that P not=NP. (7 Refs)
Subfile: B C
Descriptors: codes; cryptography
Identifiers: random cipher cracking; data encryption; security; cascade ciphers; unicity distance; plaintext attack; key lengths; time-space trade-off; permutations; exhaustive experiments; **key bits** ; nonpolynomial lower bound
Class Codes: B6120B (Codes); C6130 (Data handling techniques)

18/5/12 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

02324326 INSPEC Abstract Number: B84053424
Title: On the power of cascade ciphers
Author(s): Even, S.; Goldreich, O.
Author Affiliation: Dept. of Computer Sci., Technion-Israel Inst. of Technol., Haifa, Israel
Conference Title: Advances in Cryptology. Proceedings of Crypto 83 p. 43-50
Editor(s): Chaum, D.
Publisher: Plenum, New York, NY, USA
Publication Date: 1984 Country of Publication: USA xii+395 pp.
ISBN: 0 306 41637 9
Conference Sponsor: Int. Assoc. Cryptologic Res
Conference Date: 21-24 Aug. 1983 Conference Location: Santa Barbara, CA, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: The unicity distance of a cascade of random ciphers, w.r.t. known plaintext attack is shown to be the sum of the key lengths. A time-space trade-off for the exhaustive cracking of a cascade of ciphers is shown. The structure of the set of permutations realized by a cascade is studied; it is shown that only l*2/sup k/ exhaustive experiments are necessary to **determine** the behaviour of a cascade of l stages, each having k **key bits** . It is concluded that the cascade of random ciphers is not a random cipher. Yet, it is shown that, with high probability, the number of permutations realizable by a cascade of l random ciphers, each having k **key bits** , is 2/sup lk/. **Next** , it is shown that two stages are not worse than one, by a simple reduction of the cracking problem of any of the stages to the cracking problem of the cascade. Finally, it is shown that proving a nonpolynomial lower bound on the cracking problem of long cascades is a hard task, since such a bound implies that P not=NP. (6 Refs)
Subfile: B
Descriptors: cryptography
Identifiers: cryptography; cascade ciphers; unicity distance; plaintext attack; key lengths; cracking
Class Codes: B6120B (Codes)

18/5/13 (Item 1 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00612550 00NR10-205
Crypto proposal faces long journey -- Rijndael algorithm needs conformance, interoperability tests before implementation
Messmer, Ellen
Network World , October 16, 2000 , v17 n42 p53-59, 2 Page(s)
ISSN: 0887-7661
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Reports that the Rijndael 128-bit encryption algorithm selected by the

United States National Institute of Standards and Technology (NIST) faces conformance and interoperability tests before implementation. Explains that conformance tests would ensure that vendors implemented Rijndael properly. Mentions that **next** year, Rijndael will be officially designated the Advanced Encryption Standard (AES) to replace the 56-bit Data Encryption Standard (DES). **Indicates** that Rijndael can be used as 128-bit, 192-bit, or 256- **bit** **key** cryptography. Adds that DES can be cracked with sufficient processing power. Points out that a stronger DES called TripleDES will remain a government standard for the foreseeable future. Presents predictions that Rijndael will not appear in products for a while. Includes a sidebar. (MEM)

Descriptors: Encryption; Algorithm; Security; Federal Government; Testing; Interoperability; Standards

18/5/14 (Item 1 from file: 94)

04731003 JICST ACCESSION NUMBER: 01A0043405 FILE SEGMENT: JICST-E

Psychological Characteristics of Unsuccessful Pilot Trainees.

MATSUNAGA NAOKI (1); ASUKATA ICHIRO (1); KABASHIMA TSUKASA (1); SHIRAHAMA KYOKO (1)
(1) Japan Airlines Co., Ltd.

Uchu Koku Kankyo Igaku(Japanese Journal of Aerospace and Environmental Medicine), 2000, VOL.37,NO.1, PAGE.1-7, FIG.5, TBL.1, REF.11
JOURNAL NUMBER: Y0811AAC ISSN NO: 0387-0723
UNIVERSAL DECIMAL CLASSIFICATION: 61+
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication

ABSTRACT: Some pilot trainees can not pass flight examinations and are obliged to give up their flight training because of their insufficient technical skills. We investigated their results of group Rorschach test (a maultiple-choice test with ink blots which are similar to those for face-to-face Rorschach test). Subjects were 20 male pilot trainees (F(fail) group: mean age 22.4+-.1.5 years) who were obliged to give up their flight trainings between 1985 and 1996 because of their insufficient technical skills. The control group was made up of 125 male pilot trainees (P(pass) group: mean age 22.4.+-.1.7 years) who were the successful classmates of the unsuccessful trainees. We investigated the differences of the results of group Rorschach test given for employment screening between the two groups. All results of the scores in group Rorschach test were within normal limits both in P group and F group. There, however, were **following** **significant** differences between the two groups: (1) F group showed **more** **Key** -responses than P group (F group: 4.9.+-.2.1 P group: 3.4.+-.2.0, p<0.01). (2) F group showed more k responses than P group (F group: 0.2.+-.0.4 P group: 0.02.+-.0.1, p<0.01). (3) P group showed more FC' responses than F group (F group: 1.4.+-.1.0 P group: 2.2.+-.1.2, p<0.01). (4) F group showed more cF responses than P group (F group: 1.6.+-.1.2 P group: 1.0.+-.0.9, p<0.05). (5) P group showed higher form level than F group (F group: 120.6.+-.15.8 P group: 128.2.+-.12.6, p<0.05). The pilot trainees in F group were suggested to have vulnerability to be nervous and anxious in an inexperienced situation, to decline their ability to cope objectively and effectively with a new situation, and to increase desire for dependence upon others. (author abst.)

DESCRIPTORS: human(primates); aerospace medicine; operation(transportation); crew; personality test; projective technique(psychology); man; aptitude test; mental manifestation; comparative test; education and training
BROADER DESCRIPTORS: medicine; natural science; science; operation and driving; job classified employee; worker; psychological test; psychometry; psychiatric care; human(sociology); maleness; sex; inspection; symptom; disease; test

CLASSIFICATION CODE(S): GC12000F

18/5/15 (Item 2 from file: 94)
DIALOG(R)File 94:JICST-EPlus

04671478 JICST ACCESSION NUMBER: 00A0735398 FILE SEGMENT: JICST-E
Every company developed each next **-generation code technology for electronic commercial transaction, to propose it to ISO/IEC.**
IIZUKA MINORU (1); TONAMI SHUICHI (1); UEHARA KIYOHIKO (1); ISHIOKA TADAO (1); KATSURA KOSUKE (1); SATO AKIRA (2); (2) IBM Japan Ltd., Tokyo Res. Lab. Comp. Sci. Inst.
Denshi Joho Tsushin Gakkaishi(Journal of the Institute of Electronics, Information and Communication Engineers), 2000, VOL.83,NO.7, PAGE.590-593, FIG.6
JOURNAL NUMBER: F0019ADO ISSN NO: 0913-5693
UNIVERSAL DECIMAL CLASSIFICATION: 621.391.037.3
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Commentary
MEDIA TYPE: Printed Publication
ABSTRACT: Every company in Japan developed each **next** -generation code technology adopted by electronic commercial transaction, electronic government, and so forth using internet, to propose it to ISO/IEC of the international standardization organization. Here were introduced on the **following** code systems: 1) MARS (a system developed for **next** term common key-code standard AESin U.S.A. by IBM); 2) CIPHERUNICORN-A (a 128 bit block code developed by NEC, key selectable from 128, 192 and 256 bits, and characteristic of false key method and of use of stirring equation); 3) MISTY (total notation of 64 bit block code with 128 **bit key** -length developed by the Mitsubishi Electric Co.); 4) Hierocrypt (a 128 bit block code developed by Toshiba Corp., and characteristic of insert type SPN structure); 5) MULTI-S01 (a common key code technology developed by Hitachi Corp., and possible to detect a non-correct manipulation by inspecting redundant code preliminarily shared on encoding); 6) Camellia (a 128 bit block **next** -generation common key code colaborately developed by NTT and Mitsubishi Electric Co., which supports three kinds of key-length such as 128, 192 and 256 bits); and, EPOC and PSEC (opened key system developed by NTT, and the former lays a base on a prime factor factorization problem, and the latter lays a base on a dispersion logarithmic problem).
DESCRIPTORS: cryptogram; cryptography key; public key cryptography; data protection; computer security; ISO; IEC standard; transaction; coding(signal)
IDENTIFIERS: information security
BROADER DESCRIPTORS: protection; security; guarantee; international organization; international standard; standard(**specification**); standard; modification; signal processing; treatment
CLASSIFICATION CODE(S): ND02030R

18/5/16 (Item 3 from file: 94)
DIALOG(R)File 94:JICST-EPlus

02030775 JICST ACCESSION NUMBER: 94A0395998 FILE SEGMENT: JICST-E
Hexokinase Activity of Bovine Embryos Produced from IVM-IVF System and Their Subsequent **Development.**
RYOO Z Y (1); SUGAWARA S (1)
(1) Tohoku Univ., Sendai
Honyu Dobutsu Ranshi Gakkaishi(Journal of Mammalian Ova Research), 1994, VOL.11,NO.1, PAGE.36-42, TBL.4, REF.15
JOURNAL NUMBER: L0534ABG ISSN NO: 0916-7625
UNIVERSAL DECIMAL CLASSIFICATION: 591.3.05 636.082.4
LANGUAGE: English COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal

```
Set     Items   Description
S1       6934   ENCRYPTION()(KEY OR KEYS)
S2    1283435   STORED OR BACKUP OR BACK()UP OR STORAGE
S3      19667   PLD OR PROGRAMMABLE()LOGIC()DEVICE?
S4       2870   (KEY OR KEYS)(N)(BIT OR BITS OR BITE OR BITES OR BYTES)
S5    7235459   INDICAT? OR DETERMIN? OR SPECIF? OR SIGNIF?
S6       7352   (MORE OR FURTHER OR ADDITIONAL)(N)(KEY OR KEYS)
S7    7185403   FOLLOW? OR SUCCEED? OR NEXT OR SUBSEQUENT?
S8          0   S1 (S) S2 (S) S3
S9          0   S4 (S) S5 (S) S6
S10       833   S1 (S) S2
S11       360   S1 (5N) S2
S12        75   S4 (5N) S5
S13       163   S5 (5N) S6
S14        12   S4 (5N) S6
S15         0   S1 (S) S3
S16       250   S12 OR S13 OR S14
S17       188   S16 NOT PY>2000
S18       187   S17 NOT PD>20001128
S19       128   RD (unique items)
S20        16   S19 (S) S7
File  15:ABI/Inform(R) 1971-2004/Jun 01
         (c) 2004 ProQuest Info&Learning
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 647:CMP  Computer Fulltext 1988-2004/May W4
         (c) 2004 CMP Media, LLC
File 275:Gale Group Computer DB(TM) 1983-2004/May 31
         (c) 2004 The Gale Group
File 674:Computer News Fulltext 1989-2004/May W3
         (c) 2004 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2004/Jun 01
         (c) 2004 The Dialog Corp.
File 621:Gale Group New Prod.Annou.(R) 1985-2004/May 28
         (c) 2004 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2004/May 31
         (c) 2004 The Gale Group
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 613:PR Newswire 1999-2004/Jun 01
         (c) 2004 PR Newswire Association Inc
File  16:Gale Group PROMT(R) 1990-2004/May 31
         (c) 2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 553:Wilson Bus. Abs. FullText 1982-2004/May
         (c) 2004 The HW Wilson Co
```

20/5,K/4 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01041524 CMP ACCESSION NUMBER: OST1995012350052
Oracle Ships Encryption Software-Product Secures Data On SQL*Net 2.1 Network Going To Non-Oracle Databases (Product Briefs)
Dan Richman
OPEN SYSTEMS TODAY, 1995, n 167, PG29
PUBLICATION DATE: 950123
JOURNAL CODE: OST LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Databases & Development Tools
WORD COUNT: 324
TEXT:
Oracle has begun shipping software it said encrypts information passing over a SQL*Net 2.1 network, even if the information is directed to non-Oracle databases or uses multiple network protocols.

... software uses the RC4 algorithm, which Oracle has licensed from RSA Data Security, Redwood Shores, Calif. The **next** version of Secure Network Services (1.1), due out by April 1, will offer a choice of...

...widely used and offers more security, using a 56-bit key as compared to RC4's 40- **bit key** . But it imposes a `` **significantly** greater'' performance penalty, Jarvis said.
Secure Network Services doesn't decrypt data when it passes through Oracle...

20/5,K/5 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01824749 SUPPLIER NUMBER: 17208457 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Netscape Encrypted Data Cracked.
Newsbytes, pNEW08180023
August 18, 1995
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 679 LINE COUNT: 00056

FILE SEGMENT: NW File 649

... the financial data in the messages using 56-bit keys. Siino explained, "You can export over 40- **bit keys** for a **specific** application." The new system should be available early **next** year.
Many companies working on secure transaction systems hope the much more secure 128-bit code version...

20/5,K/6 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01511087 SUPPLIER NUMBER: 11744452 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Practical minimal perfect hash functions for large databases. (time and space saving program development techniques) (Technical)
Fox, Edward A.; Heath, Lenwood S.; Chen, Qi Fan; Daoud, Amjad M.
Communications of the ACM, v35, n1, p105(17)
Jan, 1992
DOCUMENT TYPE: Technical ISSN: 0001-0782 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 10935 LINE COUNT: 00860

ABSTRACT: Hash functions are used in artificial intelligence, data structures, data base management, file processing and information retrieval and other applications where data is accessed based on the value of a key.

Research is presented on improving current hashing practices to optimize use of time and space using a minimal perfect hash function (MPHF) whenever possible. An algorithm designed to search for MPHFs even for large static keys sets of over one million keys has been developed and its use is demonstrated. Expected uses for the algorithm include improving access to CD-ROM data as well as fast access to lexicons built from machine-readable dictionaries. The system automatically rebuilds a new MPHF when enough changes have been made to the data to warrant it.
SPECIAL FEATURES: illustration; table; chart
DESCRIPTORS: Program Development Techniques; DBMS; Hashing functions; Algorithm Complexity
FILE SEGMENT: AI File 88

... 2 to require as few bits as possible. The experiments indicated by these rows were conducted as **follows** : Lower and lower bits/key values were tried until Algorithm 2 failed to find an MPHF consistently...

...time for those runs are reported in Table 7. The run time for n = 262144 is anomalous, **indicating** that **bits / key** can actually be pushed lower.
Algorithm 2 is also capable of running efficiently using external
TABLE 6...

20/5,K/7 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01465622 SUPPLIER NUMBER: 11648794 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Specifying an electronic mail system with HP-SL. (specification language) (includes related article on the specification of state in HP-SL) (Technical)
Goldsack, Patrick C.; Rush, Tony W.
Hewlett-Packard Journal, v42, n5, p32(8)
Dec, 1991
DOCUMENT TYPE: Technical ISSN: 0018-1153 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 5747 LINE COUNT: 00518

ABSTRACT: HP Specification Language (SL) formal notations aid in developing a simple electronic mail (E-mail) system by making the user deal with system behavior issues, letting the user reason out the specifications, clarifying the system and providing unambiguous notation of behavior. The E-mail system presented has registered users, each with an in tray, an out tray and a pending tray. The users can read and delete messages from their in tray, compose messages in their pending tray and send messages from their out tray to another user's in tray. HP-SL provides the language models for users, messages and trays and deals with the operations involved. The problems with this model include its operational limitations, its lack of concurrency handling and its inability to deal with an unreliable communication medium. However, the use of the formal HP-SL in refinement shows that an abstract specification of an entire system, followed by a precise specification of one or two subsystems, is valuable.

DESCRIPTORS: E-Mail; Formal Languages; Specifications; Program Logic; System Design
FILE SEGMENT: CD File 275

... practice for whole systems (it takes too much time) but an abstract specification of a whole system, **followed** by detailed **specifications** of one or **more** **key** subsystems is practical and useful. As with reasoning about system properties, reasoning about the correctness of refinement...

20/5,K/11 (Item 3 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

04487469 Supplier Number: 57588415 (THIS IS THE FULLTEXT)
Distributed Computing Puts The Net To Work 11/12/99.
Zurcher, Anthony
Newsbytes, pNA
Nov 12, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 986
TEXT:
WASHINGTON, DC, U.S.A., 1999 NOV 12 (NB) -- SETI@home aims to tackle one of the biggest computing problems in history, so big that a $900 home computer may wind up solving it--if a $100 cell phone doesn't get there first. The Search for Extraterrestrial Intelligence at Home is the highest- profile experiment yet in "distributed computing." This approach breaks gargantuan problems into smaller segments that can be attacked with personal computers, then uses the Internet to send out these slices and collect the results. It's a rough equivalent of Tom Sawyer getting every other boy in town to whitewash the fence, one plank at a time. So far, more than 1.4 million people in 224 countries have downloaded the SETI@home software and used it to sift through the 35 gigabytes of raw data that the Arecibo Observatory radio telescope in Puerto Rico collects daily. This free program, available for Windows, Mac and Unix systems, downloads a 350-kilobyte slice of the information recorded by Arecibo's 1,000-foot-wide dish. Then, whenever the computer is idle, the program analyzes this data--a "work unit"--for unusual signal patterns, displaying the results as a "Star Trek"-ish screen saver. When finished, the program sends the information back to the SETI servers and downloads more data. Sifting through the billions and billions of bits of data that Arecibo collects is a monumental task, but on the other hand there's the chance, however slight, that your rusty old PC might be the one that first detects a signal. "The search for extraterrestrial intelligence is the biggest question that faces us, outside of how the universe began," said David P. Anderson, project director of SETI@home and a former professor at the University of California at Berkeley. "(It's) something that attracts a lot of people." That altruistic pursuit, however, isn't the only reason people are flocking to SETI@home. The site has also attracted what Anderson calls "computer hot-rod guys," who compete to see whose machines can process information the fastest. SETI@home keeps statistics on individual users and groups of users, and the results are posted in a top-1,000 list. It's a subculture all its own, and SETI@home isn't the only site where this online "sport" is being played. On Distributed.net , more than 60,000 computers are working together to win a code-breaking contest sponsored by RSA Data Security. The Bedford, Mass.-based firm, in an effort to prove the ineffectiveness of current, government-sanctioned encryption methods, is offering $10,000 to the first group that cracks a "64- **bit** " **key** (the number **indicates** the complexity of the equation behind that key). Like SETI@home, Distributed.net keeps track of how much data different teams of users are processing and ranks them accordingly. As the competition heats up, different groups with different allegiances vie for the top ranking. "People were joining together and forming teams even before we formalized the process on our server," said David McNett, president and co-founder of Distributed.net. "We have teams I never would have guessed would have an organized interest in our project: school teams, company teams, bird-watcher teams . . . anything you can imagine." Colin Hildinger, for instance, runs Team Warped, made up of people who use and support the IBM OS/2 operating system. For dedicated computer aficionados, the choice of an operating system is a very personal expression of who they are--hence the attempts to display its prowess. At Distributed.net, even the long-forgotten Amiga platform has a team competing for the prize. "We know that the odds of our team winning aren't that great," Hildinger wrote in an e-mail. "Currently the odds are about one in 100 that Team Warped will find the key, and the odds that it will actually be an OS/2 machine are much worse. But every OS/2 user involved would love to have the name OS/2 somehow associated with winning one of these contests." In the meantime, one of Hildinger's main concerns is that his team stay ahead of Team Win32, the Windows group. Nobody, it seems, wants to see Microsoft win--online or

in the courts. But none of these teams is likely to crack this problem any time soon, as only 15 percent of the possible solutions have been checked since the contest began Oct. 22, 1997. Hildinger noted that this could be a problem: "When the current project looks like it will drag on for years and future projects are vaporware, it's hard to get motivated to do anything." The site does have other computing projects on the horizon, however, including a variety of cryptological and mathematical problems. More interesting, but less likely, is the possibility that the rendered animation for the **next** "Toy Story" movie could be done over the Internet. McNett said the big obstacle there isn't technology, but copyright-protection issues. As for the SETI@home project, Anderson predicted it would be completed within two years, assuming no signals from extraterrestrials are found before then. After that, the group plans to start analyzing recordings from a telescope in Australia, covering radio sources in the Southern Hemisphere sky. And faster DSL and cable-modem connections could make many other projects possible. "There may be approaches to finding a cure for cancer that are computational," Anderson said. "We could use computers to simulate the way that drugs might work. Another possible project involves the simulation the ecology of the planet, predicting global warming. A lot of areas of science are starting to replace laboratories with computers." And it need not just be traditional computers doing the work. Already, Anderson has been in contact with someone interested in running SETI@home on his Nokia cellular phone. He said, "They're going to be putting computers into everything, so you might someday have your toaster oven doing scientific projects while it isn't in use." Reported By Newsbytes.com, http://www.newsbytes.com .
(19991112/WIRES ONLINE/)

PUBLISHER NAME: Newsbytes News Network
INDUSTRY NAMES: BUSN (Any type of business); CMPT (Computers and Office Automation); TELC (Telecommunications)

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...current, government-sanctioned encryption methods, is offering $10,000 to the first group that cracks a "64- **bit** " **key** (the number **indicates** the complexity of the equation behind that key). Like SETI@home, Distributed.net keeps track of how...and mathematical problems. More interesting, but less likely, is the possibility that the rendered animation for the **next** "Toy Story" movie could be done over the Internet. McNett said the big obstacle there isn't...

20/5,K/13 (Item 5 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

02828686 Supplier Number: 45735975 (THIS IS THE FULLTEXT)
Netscape Encrypted Data Cracked 08/18/95
Newsbytes, pN/A
August 18, 1995
Language: English Record Type: Fulltext
Document Type: Newswire; General Trade
Word Count: 652
TEXT:
TOKYO, JAPAN, 1995 AUG 18 (NB) -- Two computer users have managed to break Netscape's Secure Sockets Layer (SSL) encryption code in response to a challenge posted to the Internet. But far from scare people away from using the system for online purchases, the results could reassure people of the safety.

In mid July Hal Finney, a US computer user, posted data in an Internet message that he recorded when he sent an order, containing a fake name and credit card details, to Netscape's own computer. Setting a task for the hacking community, he wrote, "The challenge is to break the encryption and recover the name and address info I entered in the form and sent securely to Netscape."

Early this week, news came from Damien Doligez, a French computer user, that he had cracked the code and revealed the contents of the message. Several hours later a message from an American team also claimed the same feat, actually cracking it two hours earlier than Doligez.

While the results look damaging on the surface, Netscape, and Doligez, pointed out the amount of computer processing power needed to hack just one message and the difficulty in repeating the process.

Roseanne Siino of Netscape told Newsbytes, "The real issue is whether this compromises security on the net. He used 120 computers for 8 days just to crack one message." Siino points out that to break into another message would require another eight days at the same 120 workstations and 2 parallel computers.

In home computer terms, Doligez guesses a network of about 80 Intel Pentium-based machines would be equivalent to the system he had access to via his workplace, INRIA in Paris, and computers an Ecole Polytechnique and ENS.

Netscape estimates the total cost of this computing time at around $10,000, meaning there are many more economical ways of getting credit cards numbers than hacking into Netscape SSL messages.

Doligez agrees, writing on his home page: "The technical implications are almost zero. Everybody who understands the technical details knew perfectly well that this was do-able and even easy. You have to understand what happened exactly. I did not break SSL itself. I did only break one SSL session that used the weakest algorithm available in SSL. If I want to break another session, it will cost another 8 days of all my machines."

The vulnerability of the encryption system is shown by its international use. The coding system available via Netscape software from the Internet makes use of a 40-bit encryption key. A stronger version, using a 128-bit key, is available to US citizens but restricted from export outside the United States by government regulations.

Netscape's Siino explained the US government allows export of the lower security version "because they can break it."

There are some hopes that this demonstration will help persuade the US government to lift export restrictions on some harder-to-crack versions of the code.

Netscape is currently developing a new Secure Courier code which just encrypts the financial data in the messages using 56-bit keys. Siino explained, "You can export over 40- **bit keys** for a **specific** application." The new system should be available early **next** year.

Many companies working on secure transaction systems hope the much more secure 128-bit code version of the system will be available for export eventually. This is said to be almost unbreakable, requiring a trillion times more processing power to crack than the 40-bit version.

Internet users can view a copy of the original challenge, access Doligez's home page with details of his result, get copies of the program used to crack the code and read Netscape's response to the news through a special section at Netscape,
http://home.netscape.com/newsref/std/key_challenge.html

(Martyn Williams/19950818/Press contacts : Roseanne Siino, Netscape, +1-415-528-2619 , Internet email roseanne@netscape.com; Damien Doligez, Internet email damien.doligez@inria.fr ; Hal Finney, Internet email hfinney@shell.portal.com

PUBLISHER NAME: Newsbytes News Network
COMPANY NAMES: *Netscape Communications
EVENT NAMES: *350 (Product standards, safety, & recalls)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *7372691 (Data Encryption Software)
INDUSTRY NAMES: BUSN (Any type of business); CMPT (Computers and Office Automation); TELC (Telecommunications)
NAICS CODES: 51121 (Software Publishers)

... the financial data in the messages using 56-bit keys. Siino explained, "You can export over 40- **bit keys** for a **specific** application." The new system should be available early **next** year.

Many companies working on secure transaction systems hope the much

more secure 128-bit code version...

20/5,K/14 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

06994465 Supplier Number: 58170737 (USE FORMAT 7 FOR FULLTEXT)
EPL, Commercial Crime, Construction Cover. (Brief Article)
Risk Management, v46, n12, p66
Dec, 1999
ISSN: 0035-5593
Language: English Record Type: Fulltext
Article Type: Brief Article
Document Type: Magazine/Journal; Trade
Word Count: 623
PUBLISHER NAME: Risk Management Society Publishing, Inc.
COMPANY NAMES: *Broker London Special Risks
EVENT NAMES: *366 (Services introduction)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *6300000 (Insurance)
INDUSTRY NAMES: BUSN (Any type of business); INSR (Insurance and Human Resources)
NAICS CODES: 524 (Insurance Carriers and Related Activities)
SPECIAL FEATURES: INDUSTRY; COMPANY

... including law firms, medical and dental offices, architecture and engineering firms and small manufacturers. The product will **specifically** address **more** **key** market areas **next** year. For more information, call 847.320.5593.
Commercial Crime
Employee dishonesty can have a devastating effect...

20/5,K/15 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

03726227 Supplier Number: 45282382 (USE FORMAT 7 FOR FULLTEXT)
Oracle Ships Encryption Software
Open Systems Today, p29
Jan 23, 1995
ISSN: 1061-0839
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 344
PUBLISHER NAME: CMP Publications, Inc.
COMPANY NAMES: *Oracle Corp.
EVENT NAMES: *330 (Product information)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *7372600 (Computer Network & Communications Software)
INDUSTRY NAMES: BUSN (Any type of business); CMPT (Computers and Office Automation); LAW (Law)
NAICS CODES: 51121 (Software Publishers)
TICKER SYMBOLS: ORCL
SPECIAL FEATURES: COMPANY

... software uses the RC4 algorithm, which Oracle has licensed from RSA Data Security, Redwood Shores, Calif. The **next** version of Secure Network Services (1.1), due out by April 1, will offer a choice of...

...widely used and offers more security, using a 56-bit key as compared to RC4's 40- **bit** **key** . But it imposes a " **significantly** greater" performance penalty, Jarvis said.
Secure Network Services doesn't decrypt data when it passes through Oracle...